MARINE AVIATION & TRANSPORT INSURANCE REVIEW

A cura di: *Cristina Castellini, Responsabile Trasporti e Aeronautica - ANIA Associazione Nazionale tra le Imprese Assicuratrici*

SOMMARIO

ottobre 2017 - N. 4 anno VII

Marine & Transport

Marine e Cyber Risk 3
di *Paolo Lovatti*

Cyber Risks in the Marine environment: an international approach from an Italian observer 13
di *Alberto Batini*

Aviation

Aviation Cyberspace Liabilities and Insurance 23
by *Anna Masutti, Roland Kuesters, Roger Sethsson*

Lo stato dell'arte nella ricerca applicata alla sicurezza aerea in Europa 30
di *Doriano Ricciutelli*

Rischio Paese

Gli USA verso una politica unilaterale delle sanzioni? Il Congresso vara il CAATSA contro Russia, Iran, Corea del Nord (e Trump) 37
di *Paolo Quercia*

MARINE AVIATION & TRANSPORT INSURANCE REVIEW

Dal 19 al 20 settembre si è svolta a Tokyo la 143ª edizione dello IUMI la Conferenza mondiale degli assicuratori *Marine*, che ha coinciso con il centenario della fondazione della General Insurance Association of Japan (GIAJ) .

A COMPREHENSIVE GLANCE ON THE MARINE, AVIATION & TRANSPORT WORLD

The idea is to supply and update our associates with the latest legislative juridical developments at a national and European level. Our aim is to present the information in a way that is easy to access and use. We believe that this newsletter will fill an important gap due to the fact that most journals and legal reviews are often complex and it takes a lot of time to find the information required by insurance staff.

DISCLAIMER

The objective of the Review is to inform its readers and not to suggest underwriting practices or other behaviours which may affect competition or restrain from acting accordingly to the applicable national competition and antitrust laws and to the European competition legislation. Whilst every care has been taken to ensure the accuracy of the papers and articles at the time of publication, the information is intended as guidance only. It should not be considered as legal advice.

MARINE AVIATION & TRANSPORT INSURANCE REVIEW

MARINE E CYBER RISK

Paolo Lovatti
Global Marine Consultant

Il 90% circa del trasporto mondiale di merci è effettuato via mare, con le navi, le rotte e i porti che possono essere immaginati come le arterie principali dell'economia globale dalla quale ormai tutti siamo circondati.

I porti in generale e i loro container terminal dipendono sempre di più da sistemi di comunicazione e gestione elettronica che permettono di semplificare e velocizzare le operazioni di imbarco/sbarco, lo stoccaggio e l'inoltro delle merci. E' evidente che qualsiasi errore o disfunzione dei sistemi di gestione IT può causare gravi disservizi in catene di approvvigionamento sempre più complesse.

Il processo di digitalizzazione dei sistemi di gestione delle navi è altrettanto incessante sia a livello di navigazione che di controllo della propulsione e di tutti i sistemi di bordo.

L'aspetto negativo di questa costante evoluzione tecnologica, se non correttamente valutata e controllata, è che questo cambiamento è inevitabilmente destinato a creare rischi sempre maggiori nel caso di accessi non autorizzati ai sistemi elettronici di gestione o di attacchi dolosi ai sistemi stessi o alle reti. Occorre tener presente che questi attacchi possono provenire da più fonti con scopi molto diversi:

- attivisti politici o ex-dipendenti che intendono screditare istituzioni e aziende con la pubblicazione, o comunque la divulgazione, di dati sensitivi;

- gruppi criminali le cui azioni sono volte allo spionaggio commerciale o industriale oppure condotte oggi sempre più mirate ad ottenere riscatti a fronte del rilascio di codici di decrittazione dei sistemi bloccati dal *ramsonware*;
- Stati o organizzazioni terroristiche, sostenute anche da Stati, che hanno lo scopo di creare panico, discredito, effettuare azioni di spionaggio o comunque arrecare danni alle infrastrutture critiche dei Paesi nemici e alle relative economie.

L'attacco recentemente subito dalla compagnia danese di navigazione AP Moller-Maersk S/A (APM), il più importante vettore nel trasporto di container e di general cargo, che controlla circa il 18% dei traffici mondiali, è la dimostrazione che anche il mondo marittimo non è esente dai rischi cibernetici. Il malware chiamato dai ricercatori GoldenEye o Petya o NotPetya ha iniziato a diffondersi martedì 27 giugno in Ucraina andando poi a colpire decine di società in diverse parti del mondo.

Maersk ha dichiarato di essere stata inizialmente danneggiata dall'infezione il successivo 28 giugno; il virus si è poi propagato praticamente in tutti i suoi terminal dislocati in 76 Paesi nel mondo, in modo più o meno profondo.

NotPetya è un *worm* distruttivo auto propagatore in grado di diffondersi rapidamente attraverso reti di computer scarsamente protette, paralizzando i computer ad esse collegati, impiegando la crittografia dei dischi rigidi in maniera tale che l'hardware non possa più funzionare.

Il terminal maggiormente colpito è stato quello di Rotterdam Maasvlakte II che nei primi giorni successivi all'attacco è stato in grado di operare solo al 15% del suo potenziale. Il blackout è durato diversi giorni durante i quali APM ha potuto gestire le operazioni di imbarco/sbarco ricorrendo a modalità tradizionali. Solo il 9 luglio APM è stata in grado di riprendere totalmente il controllo in tutti i suoi terminal.

Durante questo periodo all'interno del gruppo era stato imposto l'obbligo di non aprire eventuali allegati di e-mail di cui non fossero sicuri la provenienza e il contenuto, nel timore di nuove infezioni.

Nei primi giorni dell'attacco era difficile sapere, per APM e per i caricatori, dove i carichi si trovassero causando un panico fino a quel momento imprevedibile ed un allarme tanto più accentuato quanto la catena logistica dei clienti prevedeva ridotti margini di tempo per il ritiro e la distribuzione delle merci.

Nei giorni successivi, a seguito dei piani di *recovery* messi immediatamente in atto, la situazione è tornata gradualmente sotto il pieno controllo di Maersk che anche nei momenti di maggior criticità, pur ammettendo le difficoltà nella riconsegna dei carichi e nell'accettazione di nuove caricazioni, ha sempre dichiarato che il controllo delle navi e le comunicazioni con gli equipaggi non erano mai state messe a rischio o pregiudicate dall'attacco.

Al momento risulta difficile stabilire quali saranno gli effettivi costi, diretti e indiretti, a carico di Maersk.

Le prime indicazioni fornite da Maersk riportano che la capacità di carico nella settimana successiva all'attacco ha avuto un'importante flessione passando da 210.000 a 160.000 container di 40'.

I costi economici sono stati stimati in US$ 850 milioni.

Si calcola che le società del Gruppo con le loro collegate gestiscano globalmente circa 3.300 TEU all'ora con entrate per US$ 2.700.000.

Resta il fatto che, in base a un'indagine globale di settore effettuata da consulenti nella sicurezza informatica, è risultato che oltre il 44% delle linee di navigazione analizzate mostra livelli di sicurezza ridotti in relazione all'applicazione di elementi basilari nella protezione dei sistemi.

Nel corso dell'analisi è stato messo fra l'altro in evidenza che la maggior parte dei principali vettori marittimi permette ai rispettivi caricatori di servirsi delle proprie piattaforme elettroniche di accesso, utilizzando "x" o "12345" come password, ammettendo di fatto un libero accesso alle stesse a clienti e a criminali senza distinzione.

Un aspetto altrettanto importante nel contesto dei *cyber risk* e della protezione dei sistemi informatici, riguarda la tutela dei sistemi elettronici delle navi, anch'essi potenzialmente oggetto di intrusioni da parte del *cyber crime*.

Al momento i casi conosciuti e certi nei quali gli hacker possono aver messo a repentaglio la sicurezza della navigazione sono limitati ma indicativi. Il settore marittimo comunque già da alcuni anni ha cominciato a interrogarsi sui potenziali rischi e il Maritime Safety Committee dell'IMO – International Maritime Organization - con la circolare MSC-FAL.1/Circ.3 ha predisposto una serie di avvertenze sui cyber risk marittimi.

Esse forniscono indicazioni e raccomandazioni di massima agli armatori e agli operatori sugli specifici rischi propri del settore, al fine di proteggere la navigazione nel contesto delle attuali conoscenze e di quelle che si potrebbero venire a sviluppare nel prossimo futuro.

BIMCO - Baltic and International Maritime Council - la più importante associazione internazionale nello shipping, presente in oltre 120 Paesi nel mondo e i cui armatori controllano circa il 65% del tonnellaggio navigante, ha avviato parallelamente una propria analisi al fine di individuare le più importanti e specifiche vulnerabilità delle navi al fine di fornire ai propri associati indicazioni pratiche per incrementare la cyber security. Carenze significative sono state individuate nei principali sistemi utilizzati per la navigazione: GPS (Global Positioning System), AIS (Marine Automatic Identification System) e ECDIS (Electronic Chart Display and Information System).

Il sistema AIS, che si stima sia al momento istallato su oltre 400.000 navi di diverso tonnellaggio, è il miglior sistema attualmente utilizzato per evitare le collisioni in mare, è di supporto agli equipaggi per la navigazione e utilizzato per eventuali indagini in caso di incidenti. Il sistema è così preciso e di facile utilizzo che si ritiene venga fraudolentemente utilizzato anche dai pirati somali per individuare le navi da attaccare.

Al momento ci sono scarse segnalazioni di sistemi GPS o altri sistemi di supporto alla navigazione che siano stati oggetto di specifici attacchi da parte di hacker. Lo scorso anno le autorità della Corea del Sud hanno dichiarato che un importante numero di pescherecci era stato costretto a un rientro in porto anticipato a seguito di interferenze sul sistema GPS causato da hacker della Corea del Nord che, peraltro, aveva prontamente smentito l'illazione.

Nel momento in cui il segnale GPS non risulti disponibile, il comandante della nave perde il principale strumento automatico di navigazione e la maggior parte dei sistemi di collegamento.

In considerazione di ciò il comandante è costretto a rallentare la velocità, passando a modalità di navigazione a controllo manuale che può comportare ritardi e la perdita di attracchi programmati.

Uno scenario più drammatico, a seguito di un attacco, ipotizza invece la possibile collisione fra navi non più sotto controllo, con la conseguente perdita della nave, del carico e anche di vite umane, senza dimenticare i possibili disastri ambientali che ne potrebbero derivare nel caso nell'incidente fossero coinvolti dei tanker.

E' un dato indiscutibile che anche le navi fanno sempre più affidamento su sistemi che coinvolgono digitalizzazione e processi di integrazione e automazione. Anche essi non possono prescindere dalla necessità, per un loro corretto utilizzo, di una attenta gestione dei rischi cibernetici non diversa da altri sistemi di terra. La continua evoluzione dell'Information Technology (IT) e dell'Operational Technology (OT), sempre più fra loro collegate, e le necessarie connessioni a internet rendono evidente che anche le navi sono parte dell'intero sistema, con tutti i problemi che ne possono derivare.

Sinteticamente le linee guida predisposte da BIMCO, facoltative e non obbligatorie, sono predisposte per:

- far crescere la consapevolezza degli armatori sui rischi commerciali, della sicurezza e della tutela dei dati nel momento in cui le specifiche misure minime di sicurezza suggerite non siano in essere;
- proteggere da attacchi esterni i sistemi IT e OT a bordo delle navi e le attrezzature ad essi collegati;
- coordinare in maniera corretta tutto il personale che utilizza i sistemi, fornendo loro le corrette modalità di accesso alle informazioni di pertinenza;
- proteggere i dati presenti a bordo della nave in base al loro livello di sensibilità;
- proteggere le comunicazioni e lo scambio binario di dati tra navi e stazioni di terra.

Al fine di avere concreti parametri di riferimento nello sviluppo delle linee guida, BIMCO ha impiegato gli standard utilizzati dal National Institute of Standards and Technology, US Department of Commerce (NIST). Questo ha facilitato una miglior identificazione e prioritizzazione delle azioni necessarie per la riduzione nei rischi nella sicurezza cibernetica.

Il NITS identifica il *cyber risk* come il *risk of financial loss, disruption or damage to the reputation of an organization due to any sort of failure of its information technology system.* Una definizione molto stringata ma non per questo poco efficace.

Occorre mettere in evidenza che i piani e le procedure per il controllo dei rischi cibernetici dovranno essere complementari alle correnti norme generali in materia di sicurezza della navigazione contenuti nell'ISM Code e nell'ISPS Code che non subiscono modifiche.

Per una corretta gestione dei rischi, la gestione a livello di Compagnia di navigazione non si dovrà limitare alla sicurezza informatica delle singole navi, ma avrà la necessità di ampliare l'analisi e l'implementazione all'intera amministrazione di terra e a tutto il personale a bordo che abbia accesso ai sistemi.

Per un corretto approccio alle problematiche, lo sviluppo, la comprensione e la consapevolezza degli aspetti chiave della sicurezza e protezione cibernetica dovrebbero essere racchiusi per ciascun armatore, ma non solo, in un circolo virtuale che abbia inizio dalla comprensione delle minacce cibernetiche per passare alla determinazione dei rischi derivanti e per concludersi con lo sviluppo dei piani contingenti per la riduzione dei rischi.

In particolare appare necessario:

- identificare i rischi derivanti dall'esterno che possano compromettere la sicurezza della nave e della sua navigazione, unitamente a quelli interni dipendenti dall'uso improprio dei sistemi o dalla loro obsolescenza;
- individuare le vulnerabilità con un inventario dei sistemi elettronici di bordo che siano direttamente o indirettamente collegati fra di loro. Sulla base di questa classificazione comprendere quali potrebbero essere gli effetti di un'intromissione non autorizzata;

- determinare la possibile esposizione di rischio a seguito sia di un attacco esterno, sia di un uso improprio interno. Sarà importante che questa valutazione venga effettuata sui singoli sistemi e sulla possibile propagazione derivante dall'interconnessione fra gli stessi;
- sviluppare misure di protezione e controllo al fine di ridurre le vulnerabilità e l'impatto che un attacco doloso o un utilizzo improprio potrebbe avere;
- fissare specifici piani contingenti per essere in grado di rispondere in maniera adeguata ai problemi che potrebbero sorgere a seguito di un *malware* e permettere alla nave di continuare a navigare in maniera sicura e adeguata;
- essere in grado di utilizzare e mettere in pratica i piani di risposta ad un attacco e valutare l'impatto effettivo che essi potrebbero avere sui sistemi, anche per meglio comprenderne la vulnerabilità in un'ottica di esperienza futura e di prevenzione.

Il processo che dovrà essere sviluppato da ciascun armatore, consapevole dei sempre maggiori rischi a cui la flotta è sottoposta, non è semplice e dovrà essere condiviso con specialisti del settore.

Basti pensare che per quanto riguarda l'individuazione delle vulnerabilità, se ci si limita alla nave, le principali aree di intervento dovranno essere focalizzate su questi sistemi:

- gestione del carico. I sistemi digitali utilizzati per la gestione e il controllo dei carichi, inclusi quelli pericolosi, possono interfacciarsi con molti sistemi informatici di terra. I sistemi possono includere strumenti messi a disposizione del caricatore per conoscere la posizione del suo carico, utilizzabili via internet. Queste possibilità di interfaccia, è ormai noto, sono un area di alta vulnerabilità agli attacchi in tutte le fasi in cui il carico resta sotto la responsabilità dell'armatore, dal momento dell'imbarco alla riconsegna delle merci compresa l'emissione delle B/L e la predisposizione dei manifesti di carico;
- ponte di comando. Il continuo incremento nella digitalizzazione dei sistemi di navigazione interfacciati con i network di terra che provvedono ad aggiornare continuativamente i dati necessari, rendono anche questi sistemi vulnerabili ad attacchi di

qualsiasi tipo. Un'azione dolosa potrebbe estendersi fino a rendere il controllo della nave difficile o impossibile, andando a interferire con i sistemi ECDIS, GPS/GNSS, AIS, VDR e radar/ARPA;

- apparati di propulsione, generatori e impianti in generale. Anche in questo caso ci si trova di fronte ad una digitalizzazione sempre più avanzata degli apparati, utilizzata per ottimizzare la navigazione, limitare i consumi e ridurre gli equipaggi. La vulnerabilità sarà tanto più elevata quanto maggiore sarà l'integrazione tra questi sistemi e quelli del ponte di comando;
- controllo degli accessi. Sono i sistemi di prevenzione utilizzati per supportare il controllo degli accessi e garantire la sicurezza materiale di passeggeri ed equipaggi nelle diverse parti della nave, soprattutto se da crociera;
- gestione e servizi per i passeggeri. Sono i dispositivi che permettono di gestire imbarchi/sbarchi di passeggeri, il loro controllo a bordo utilizzandone anche i relativi dati sensibili. L'utilizzo da parte del personale di bordo di tablet, scanner o palmari per questa gestione può aumentare i rischi di infiltrazione di *malware*;
- network pubblici a disposizione dei passeggeri. Le reti fisse o wireless collegate a internet istallate a bordo a beneficio dei passeggeri sono di difficile controllo e non dovranno pertanto avere connessioni dirette o indirette con qualsiasi altro sistema critico di bordo per la navigazione;
- network per il governo in genere della nave e del personale di bordo. I sistemi di bordo utilizzati per il governo della nave divengono anch'essi particolarmente sensibili quando sono collegati via internet;
- altri sistemi di comunicazioni in genere. Anche in questo caso la connessione a internet via satellite o con altre modalità wireless rende la nave particolarmente sensibile a eventuali attacchi. Sarà pertanto necessario individuare le possibili interconnessioni tra questi sistemi e gli apparati generali di controllo della nave.

In questo contesto, le maggiori vulnerabilità sulle quali gli armatori avranno la necessità di intervenire sono principalmente identificabi-

li nei sistemi operativi obsoleti, negli antivirus non istallati o superati, nei network scarsamente segmentati, nel carente utilizzo di password, nel controllo degli accessi da parte di terzi estranei alla navigazione, insufficiente o non adeguatamente verificato.

Nel processo di controllo e mitigazione dei rischi, una volta identificate le vulnerabilità e implementate le prevenzioni, un aspetto altrettanto importante sarà quello di procedere con la formazione del personale di bordo per renderlo consapevole che i rischi cibernetici, anche se non immediatamente percepibili, rappresentano un'area in cui questo tipo di sicurezza ha lo stesso valore di tutti gli altri rischi materialmente riconoscibili e percepibili.

In conclusione alcune considerazioni:

- le problematiche legate agli attacchi e ai rischi cibernetici in generale sono ormai una realtà anche dell'industria marittima;
- in una parte degli armatori non vi è ancora la piena consapevolezza dei rischi, ma la realtà pone ormai tutti di fronte a scelte difficilmente rinviabili;
- l'applicazione delle linee guida predisposte da BIMCO può consentire una riduzione delle vulnerabilità nel mondo marittimo permettendo agli armatori di meglio conoscere i rischi e provvedere alla loro mitigazione;
- le navi e le compagnie di navigazione sono vulnerabili nella stessa misura di qualsiasi altro utilizzatore di sistemi digitali e lo possono essere ancor di più nel momento in cui il cyber crime si renderà conto che le difese sono basse o inesistenti;
- tutta la filiera del trasporto è a rischio e a questo riguardo il caso Maersk è emblematico: la possibilità di operare per aumentare le sicurezze è ampio. L'unico soggetto che ha scarse possibilità di intervento nel contenimento di questi rischi resta il proprietario delle merci cui non resta da fare altro che affidarsi alla professionalità e alla selezione degli operatori del trasporto da considerare nelle diverse fasi della catena della distribuzione.

Il mercato assicurativo *marine* non è in questo momento preparato ad assicurare i cyber risk. Con la Cyber Attack Exclusion Clause del novembre 2003, adottata dalla maggior parte degli assicuratori di

tutto il mondo, si è messo in una posizione di difesa escludendo in pratica perdite, danni, responsabilità e relativi costi derivanti da attacchi informatici in genere.

Ciò potrebbe sembrare una precisa volontà del mercato di ignorare una situazione contingente avvertita da altre linee di rischio che in questi ultimi anni hanno stimolato e proposto ai clienti "di terra" valide coperture per questa tipologia di rischio.

Il mercato di riferimento, in rapida crescita, dimostra quanto questi assicuratori siano stati in grado di anticipare i tempi ed essere preparati ad affrontare oggi situazioni che solo pochi anni fa erano solo lontanamente ipotizzabili.

Se guardiamo all'assicurazione *Hull,* gli effetti della clausola non lasciano alcuno spazio per poter reclamare agli assicuratori qualsiasi sinistro causato o derivante, totalmente o parzialmente, direttamente od indirettamente dall'uso o dall'impiego al fine di arrecare danno, di qualsiasi computer, sistema informatico, programma informatico, codice software malevolo, virus o processo informatico o di qualsiasi altro sistema elettronico.

Non è escluso e sarebbe auspicabile che a fronte di questa nuova situazione di fatto si possano aprire nuovi tavoli di confronto per la copertura dei *marine cyber risk*. L'assicurazione dei rischi *on shore* a distanza di dieci anni ha maturato un'adeguata esperienza che potrebbe essere il punto di partenza per sviluppare coperture specifiche per il settore *Hull*.

Per quanto riguarda le coperture offerte dai *P&I* usualmente esse non prevedono esclusioni specifiche dei rischi cibernetici come nell'assicurazione danni, ma la posizione e l'interpretazione potrebbe non essere così netta e avrebbe la necessità di essere meglio definita.

Sarà interessante osservare se sarà il mercato, recepite le nuove aree di rischio, ad offrire per primo e in modo proattivo le relative coperture o se esso opererà in maniera reattiva a fronte delle richieste provenienti dagli armatori ormai consapevoli dei nuovi rischi che essi devono affrontare senza alcuna salvaguardia di *Risk Transfer*.

CYBER RISKS IN THE MARINE ENVIRONMENT: AN INTERNATIONAL APPROACH FROM AN ITALIAN OBSERVER

Alberto Batini
Partner at BTG Legal (Milan)

PREAMBLE

Italy gains eight positions in the world ranking of the countries mostly cyber attacked, positioning itself now at the 42nd place.

Most popular recent threats include:

- RoughTed (large scale malvertising to spread damaging web sites and ransomwares)
- Conficker (worm targeting Windows operational systems)
- Nivdort (a trojan family also targeting Windows platforms).

The risk of cyber-attacks in the transport and marine industry increase of 15% between 2016 and 2017. Last year, according to the Italian Data Protection Authority, it generated damages for 9 Billion Euro.

Only 20% of Italian domestic companies invest in cyber security notwithstanding the clear increase of the threat.

After the global attack of Wannacry, on 27th June 2017 the Danish group AP Moeller Maersk confirmed having been severely affected by a cyber-attack. The virus name is NotPetya, a ransomware generated through the MeDoc, an accounting software largely used in Ukraine, country from where the infection spread and the most affected by the virus (78% of the notifications).

Italy is the second most affected country with 10% of notifications. Banks, Electric utility companies and shipping and transport companies have been largely targeted and affected.

A.P. Møller – Mærsk confirmed the attack but underlined that "ships remained maneuverable, communications were regular and crews safe".

The parent group APM Terminals, however, suffered heavy service disruptions at several ports (at least 17 branches worldwide including Rotterdam, a strategic hub for fruit and vegetables distribution in Europe).

KEY ISSUES

I have identified seven major key areas of cyber relevance in the marine industry (port, terminals and ship system). These have cyber threat exposures and, consequently, a cyber insurance relevance.

1. Pipelines and infrastructures protection

- According to a report from McKinsey & Co the infrastructure's congestion costs to Europe 1% of the EU GPD
- At global level $400bn per year could be saved through a better management of the existing infrastructures
- The total maritime and port industry market has an estimated growth rate of 4.7% until 2020
- If the 4 keys for the Port of Future are "size, speed, smart and sustainable", technology owns at least the last 3 and is the best tool to create value for all the stakeholders involved.

2. Cyber Protection & Intelligence for maritime safety

On 1 June 2016, IMO issued the Circular n. MSC.1/Circ.1526 providing Interim guidelines on maritime cyber risk management and addressing a number of issues.

The following problems have been found on board container ships and tankers to make these vessels more vulnerable to cyber-attack.

These include:

- Bridge systems connected to unsecure connections
- Missing software patches
- USBs passed between multiple ship computers and bridge equipment
- Unconnected firewalls
- Lack of network segregation
- Unencrypted emails
- No malware scanning on ECDIS.

The technology group Wärtsilä has taken a further important step towards developing its Smart Marine capabilities by successfully testing the remote control of ship operations. The testing, which involved driving an 80 metre platform supply vessel (the "Highland Chieftain"), through a sequence of manoeuvres using a combination of Dynamic Positioning (DP) and manual joystick control, was carried out on August 21 off the North Sea coast of Scotland in collaboration with Gulfmark Offshore, the U.S. based operator who provided the vessel for the project. Although the test vessel was in the North Sea, the remote control navigating was carried out from the Wärtsilä office located in San Diego, California, 8000 km (5000 miles) away.

Most importantly, the Wärtsilä testing was carried out using standard bandwidth onboard satellite communication. No land-based technology was used for the communications between the vessel and the remote operator workstation.

The technology is therefore available to guide a vessel remotely and this is obviously a potential target for hacker and cyber-criminal organizations.

IMO has given ship-owners and managers until 2021 to incorporate cyber risk management into ship safety, giving the industry another issue to deal with.

Owners risk having ships detained if they have not included cyber security in the ISM Code safety management on ships by 1 January 2021.

Some Classification societies expressed doubts about the ability to comply with the above deadline.

Changes to the ISM Code are required because an increasing number of vessels are found to have malware on board, which could affect ship operations and navigation safety. Controlled networks should be separated from unsecure ones, software should be patched and crew trained to prevent unintentional malware infections. Shipping companies should have layered defenses to isolate protected data from the internet, implement multi-factor authentication and retain outside security experts to help plan for a cyber-attack.

3. **Entry Exit Systems and Automated Border Control for passengers (incl. cruise passengers) and crewmembers**

These include:

- Automated gates
- face recognition
- passport reader
- mobile check points.

If a platform integrates the information of the expected boarding of vehicles and passengers based on booking records and ticketing with the data of the gates control systems, the result will be a higher automation and efficiency of gate management processes and an accurate record of all those entering or leaving a predetermined port area or zone.

4. **Evolution towards IoT, higher automation to optimize infrastructures, reduce emissions, increase multimodal operation, facilitate the information flow**

Internet of Things, or objects recognizing themselves and acquiring intelligence by communicating data about themselves and aggregate information from other sources.

Alarms warns about growing traffic ahead, medicines containers alert the patient when is the time to take them. Every object can gain an active role thanks to the web connectivity.

Ports and container terminals started to distribute sensors on cranes, transtainers, containers, tractors and gates to:

- optimize multimodal operations
- gain a better understanding and efficiency of the logistic process and management of existing infrastructures
- provide an intelligent infrastructure to optimize the information flow and efficiently manage commercial flows (reducing emissions).

Containers equipped with electronic seals could transmit operational information in advance along "intelligent" routes (id container, type of goods carried, weight, temperature during transport, data on related documentation) as well as safety information (seal intact or altered), so that terminals and competent authorities could better plan their respective follow up activities.

5. IT Platforms and clever systems to enhance safety and operational efficiency to support regional networks interconnecting port and inland hub

Last generation ships are, in fact, floating terminals up to 400 meters long carrying more than 20.000 TEU. Adapting spaces and infrastructures ashore is inevitable but while waiting for this to happen, it is crucial to remain competitive through new operational models focusing on the increase of speed of goods entry/exit logistic process.

IT Platforms and data exchange become important to optimize time and costs, but a crucial role is now assigned also to automation systems such as intelligent AGV (Automated Guided Vehicle), fast scanners, electronic seals, development of vehicle-to-infrastructure (VTI) technologies along routes connecting inland terminals, weighing systems (VGM) during handling operations. Higher is the automation level, higher is the need of an adequate cyber protection.

Terminals equipped with automated cranes and AGV increase their efficiency working h24 round the clock and increase safety on terminal areas as workers shift from outdoor areas to indoor planning and monitoring centers.

6. IT Platform, Big Data, Cloud to facilitate data exchange, process optimization and analysis for rapid and effective decisions

Valencia, Piraeus, Bremerhaven, Livorno and Ravenna participate in the "MITIGATE" project (Multidimensional, integrated, risk assessment framework and dynamic, collaborative risk management tools for critical information infrastructures) as pilot ports.

The "MITIGATE" project, started in September 2015, involves 11 partners including research and development centers and logistic institutes in ports in Germany, Italy, Spain, United Kingdom, Greece and Romania, developing new tools to manage the cyber risk. The project is co-financed by the EU Commissions in the context of the HORIZON2020 program and aims to develop an IT system, which could be used to simulate and analyze different risk scenarios to obtain more accurate projections related to levels of cyber risk in the particular sector and prevent future attacks.

Pilot ports involved in the Project are testing the system on some predetermined scenarios such as container handling and management, unloading of new vehicles from ro/ro vessels, unloading of solid bulk cargoes.

7. Sensors and information sharing

Last April, in Dallas, more than 150 typhoon-warning bells activated all together intermittently as a result of a cyber-attack. A similar attack on working orders transmitted to port cranes in a terminal or disrupting the database managing the containers position in a terminal area or the gates access permissions would be sufficient to paralyze the activity of the port.

To prevent scenarios like this the risk assessment should consider the implementation of countermeasures to protect ICT (Information & Communication technologies) and Industrial Control Systems as well as Cyber intelligence services and SCADA systems [1].

(1) Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management.

SOME PRACTICAL CONSIDERATIONS AFFECTING THE INSURANCE INDUSTRY

1. **Cyber risks policies are generally offered on claims' made terms**

Several type of malwares, such as Worms, Trojan horses, Regins, Bootkits and others, may have relatively long timeframe before becoming evident since the infection date. In such circumstances, the claim may occur months after the loss.

I would define as "target attack" the damaging consequence, which hackers sought when infiltrating the malware in the target system. This may be, for instance, a ransomware attack.

During the incubation period, the virus or malware is not really dormant but works actively scanning all the available source codes and active protocols of the affected network searching for the target protocols to activate itself. This process may take weeks or months. While doing this, the virus may easily disrupts electronic and satellite systems, discarding their usual functionality and impairing the available response of navigation systems and ship managing devices, including ECDIS, long before activating itself into the "Target attack" and generating a formal cyber claim.

The reduced functionality of navigation systems may cause other related losses and claims, which were not originally part of the target attack.

Just imagine a close headquarter colliding route of two vessels in reduced visibility where the Master is prevented from relying on GPS or other route plotting system on board because a malware is impairing system functionality while scanning source codes for active protocols in the context of a different and broader attack.

It therefore becomes crucial to draft cyber claim's made policy wordings appropriately to consider losses not directly caused by the target attack but resulting as a consequence of the virus spreading process during the incubation period (between the infection and the target attack). These may be losses which Underwriters wish to cover within the logic of the claim's made but maybe also consequences which Underwriters did not wish to cover, still

affording insurance protection against the target attack.

2. **Business interruption extended coverage including the assured's Vendors**

Is this a risk the insurance industry wish to offer an extended protection against? Some Underwriters already do so. In my opinion, this is a huge increase of the cyber risk. How much does this extended protection impact on loss statistics?

The recent "NotPetya" cyberattack that has now struck computers in at least 65 countries and severely affected Maersk, spread through an Ukrainian company's tax accounting software (according to Microsoft), which was most likely the software used by some Ukrainian vendors connected to Maersk or some Maersk's service providers. Therefore, Maersk was not directly attacked by the malware but indirectly infected following the spreading of the virus through Vendors' related systems. Many policies would not cover the business interruption damages sustained by Maersk in this case, as the infection did not hit a Maersk owned network asset. Opening up to any Vendor's related network may have an incredible huge impact on the extent of risk. There are presently no reliable statistics about the risk increase factor of such extension.

3. **Harmonizing language and policy terms**

This tends today to be fragmented. How one insurance carrier defines "computer system" or "failure of security" may differ from another, which can affect coverage.

Exclusions also varies considerably from one insurer to another. Some excludes failure to encrypt data, losses caused by gradual deterioration of computer systems or loss of money or funds, violation of consumer protection laws.

4. **Additional issues to consider**

- Self-insured retentions
- sub-limits for certain categories (like cyber extortion payments or ransomware)
- Time limitations applied to network interruption policies and retroactive dates.

5. Loss Prevention Considerations

The following areas should be increasingly developed and offered to the assureds:

- Cybersecurity risk assessments
- Proactive dark web monitoring
- Vendor security ratings
- Services to identify malicious IP addresses
- Mobile apps providing real-time threat sharing and best practices
- Online employee education and training.

CONCLUSIONS

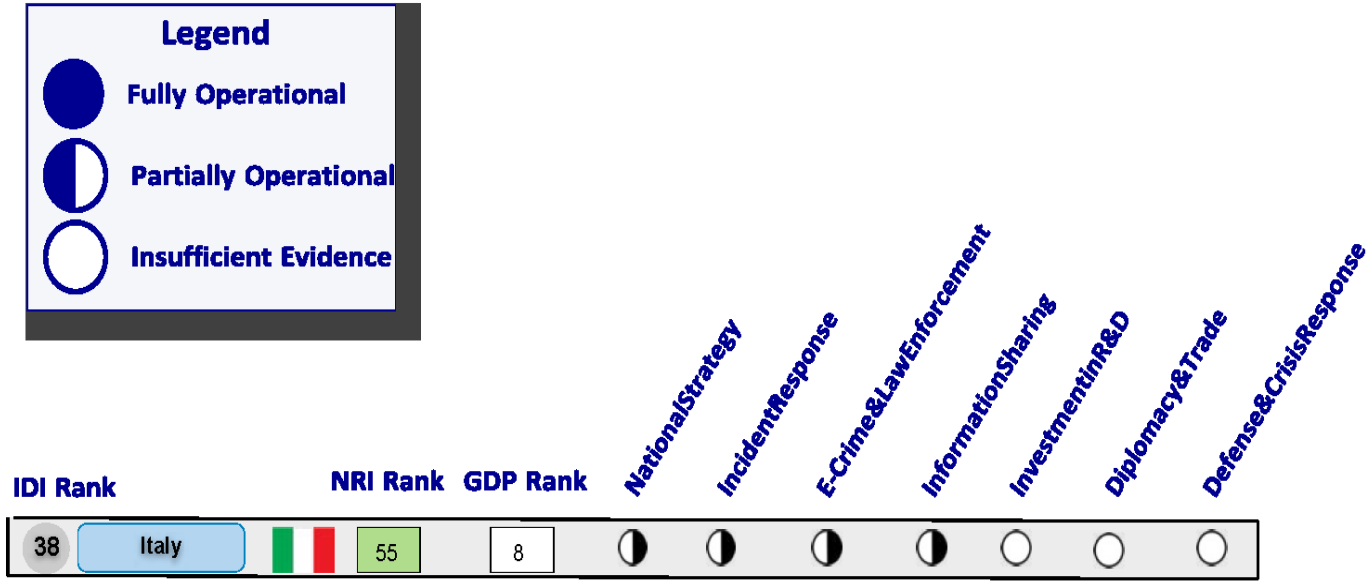
- Marine Cyber Threats are increasing and in rapid evolution
- Attacks so far targeted or involved shore logistic infrastructures
- Technology is out there and available to target and disrupt navigation systems and safety
- Non Marine Cyber Insurance Industry is progressing relatively fast to adapt
- Is the Marine Cyber Insurance Industry keeping the pace?

According to the CRI (Cyber Readiness Index) 2.0 assessment, Italy is on a path to becoming cyber ready, and is currently partially operational in many of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape while Italy continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities.

A graph about the Cyber Readiness Index in Italy is reported in the following page.

MARINE AVIATION & TRANSPORT
INSURANCE REVIEW



R&D Research & Development

Source: Potomac Institute for Policy Studies (Cyber Readiness Index 2.0 Nov 2016)

AVIATION CYBERSPACE LIABILITIES AND INSURANCE

Roland Küsters, Underwriter & Legal Counsel Aviation, Munich Re

Roger Sethsson, Head of Aerospace, Inter Hannover

Anna Masutti, Senior Partner LS LexJus Sinacta Professor of Air Law and European Transport Law at the University of Bologna

On the occasion of the last AGM event of the International Union of Aerospace Insurers that took place this year in Taormina, Sicily, some of the most significant problems with respect to the aviation cyberspace liabilities and insurance were presented. In order to understand what sort of challenges does the cybersecurity in aviation face or what are the vulnerabilities exposed at such a level, it is important to briefly define terms such as cyberattacks on aircraft systems or the critical software systems.

According to the 2017 Act introduced in the Senate of the United States regarding the Cybersecurity Standards for Aircraft to Improve Resilience, the term cyberattack is defined as the unauthorized access to aircraft electronic control or communications systems or maintenance or ground support systems for aircraft, either wirelessly or through a wired connection. Moreover, the critical software systems refer to the software systems that can affect control over the operation of an aircraft.

In an attempt to show what the response towards cyber challenges in the aviation industry should be, it is important to bear in mind some risk scenarios that conduct to an analysis of what sort of legal implications might be revealed in such cases.

As stated by the EASA Strategy and Safety Management Director Luc Tytgat in April 2017, the growing risks come from the use of new technologies and new devices: for example, pilots are increasingly using devices connected to the cockpit, such as flight maps,

and we have to guarantee these cannot be hacked. As it is the case of the United States, EASA will use information shared by the stakeholders to include cybersecurity in the Security Management System.

One of the risk scenarios that demonstrate the application of the standard clause with respect to certain cyber risks is concerned with the case of a supplier that implants a malware i.e a malicious software code into a component which is later installed by the airlines own mechanics or by a third-party MRO into an aircraft. As claimed by Raytheon's principal investigator for cyber hardening projects, Mike Worden, the malicious code could remain dormant until specific conditions are met before it is triggered, such as, for example, reaching an altitude of 10,000 feet on its 30th flight.

Another risk scenario that can take place is the one referring to a hacker flooding an airline server with so many communication requests that the server cannot carry out its normal functions. On the report of the world's leading specialist in air transport communications and information technology, SITA, in June 2015, Polish airline, LOT'S flight planning computers at its Warsaw Chopin Airport hub were overloaded. This caused cancellations of flights and delays. There are likely to have been many more similar events, but few aviation businesses openly admit to being hacked in order to not erode public confidence.

The legal challenges faced in the matter of cyberattacks on the aviation industry involve both criminal and civil implications. Due to the need of safeguarding civil aviation against cyber-threats, the Officials and representatives from the States and regional and international organizations participating in the summit on cybersecurity in civil aviation that took place in Dubai, in April 2017, declared that it is the responsibility of States to act in such a way as to mitigate the risk posed by cyber threats, to build their capability and capacity to address such threats in civil aviation, and to ensure their legislative framework is appropriately established to take action against actors of cyber-attacks.

Appreciating the wrongfulness of a cyber-attack, it does have criminal implications.

For instance, it is important to be clarified that cyber-attacks are regulated by international treaties such as the Budapest Convention on Cybercrime adopted by the Committee of Ministers of the Council of Europe in 2001 whose main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, by adopting appropriate legislation and fostering international co-operation.

It is enshrined in Article 5 of the Convention that each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data without right. International efforts to regulate cyber-attacks are essential to provide effectiveness in adopting countermeasures.

For instance, the Beijing Convention from 2010, a more recent treaty regarding the suppression of unlawful acts relating to international civil aviation, stipulates in Article 1 that any person commits an offence if that person unlawfully and intentionally destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight.

A cyber-attack may also have civil law implications.

There is a variety of questions with respect to damage and compensation that arise within the legal spectrum of such attacks. For instance, in case of a cyber-attack, damage as delay, cancellation/denied boarding, damage to baggage/cargo, costs for grounding, re-routing, information system outage, can happen.

Regarding the first set of damage (denied boarding and of cancellation or long delays), the European Union adopted the Regulation (EC) NO 261/2004 with the aim to establish the obligation of the air carrier to compensate and assist the passengers in such events. It is extremely difficult for the air carrier to avoid its liability in these cases.

For instance, in the recent case *Corina van der Lans v KLM* (2015), it

was challenging for KLM to prove that the technical problems it encountered and led to the 29 hours delay of the flight constitute an extraordinary circumstance which exonerates the air carrier from its liability. Hence, the Court ruled that a technical problem that occurred unexpectedly and which is not attributable to poor maintenance and that was not detected during routine maintenance checks does not fall within the definition of 'extraordinary circumstances'. The fact that an air carrier has complied with the minimum rules on maintenance of an aircraft cannot in itself suffice to establish that the air carrier has taken all reasonable measures within the meaning of the Regulation and, therefore, does not release it from providing care to the damaged parts.

As it is the case of a cyber-attack, we think that it could be also extremely difficult for the air carrier to prove the existence of an extraordinary circumstance and to prove that it had taken all the necessary and suitable measures to avoid the interference of the cyber -attack.

Delay is also envisaged by the Montreal Convention, signed in 1999, according to which passengers could claim compensation, but not in a fixed amount. Article 22 of the Convention provides that an airline is strictly liable up to the sum of 4,150 SDR (Special Drawing Rights) for damage specified in Article 19 sustained by a passenger as direct cause of delay or cancellation of the flight. In the event of a cyber-attack which case a delay, if the air carrier is unable to prove the provisions of Article 19, then it has to pay a compensation (not exceeding the sum of 4,150 SDR for each passenger for the damage occurred).

Regarding the damage for passenger's injuries or death, according to the provisions of the Montreal Convention, the Treaty envisages a two-tier liability system. Article 21 of the Convention provides for the possibility of the damaged part to claim up to 113,100 SDR (Special Drawing Rights) on a strict liability basis and the damaged part will not need to prove that the air carrier was at fault.

Under the fault-based liability, there is an unlimited amount and the claimant is not required to prove fault.

Under this second tier, damage above 113,100 SDR are available to

the claimant unless the air carrier is able to prove that either the damage was not caused by the negligence or other wrongful act or omission of the carrier, of its servants or agents, or was solely due to the negligence or other wrongful act or omission of a third party. Therefore, if the air carrier is unable to prove that third parties, such as the traffic controllers, were not capable of adopting adequate preventive measures, in that case the air carrier has to compensate the victims/the damaged parts without having the possibility to recover the compensation paid to the victims.

In lack of a clear legal framework with regards to cyberattacks in aviation, the various aviation organizations/institutions such as IATA (International Air Transport Association), ECAC (European Civil Aviation Conference) or EUROCONTROL (European Organisation for the Safety of Air Navigation) started to outline guidelines useful in these situations.

It is important to have a short overview about the Prudential Regulation Authority (PRA), a United Kingdom financial services regulatory body and its statutory objectives in order to notice the regulator's view with respect to aviation cybersecurity risks. PRA is part of the Bank of England and responsible for the prudential regulation and supervision of banks, insurers, investment firms in the UK.

A consultation paper with the title *Cyber insurance underwriting risk* was published by the PRA where the cyber underwriting risk is defined as the set of prudential risks emanating from underwriting insurance contracts that are exposed to losses resulting from a cyber-attack, therefore classified as a systemic risk.

According to the PRA, underwriting risks emanate both from affirmative cyber insurance policies (e.g. data breach products), but also from silent cyber risk defined as implicit cyber exposure within all risks and other liability insurance policies that do not explicitly exclude cyber risk. The loss potential of silent cyber risk is of great concern and the insurers are expected to identify, quantify and manage the risks emanating for both affirmative and silent insurance policies. Moreover, the PRA proposes that insurers should provide policyholders with greater contract certainty as to their level and type of cyber risk coverage.

Clauses relevant to cyberattacks taken into account when providing cover in respect of the ever-expanding cyber-risks are AVN48B War and Allied Perils exclusion clause with the write-back provisions AVN52 variants, the Data Recognition Exclusion clauses AVN 2000 and the corresponding write-back provisions AVN 2001 and 2002. The standard cyber insurance risks deal with liabilities for breach of intellectual property or privacy rights, loss of data, cyber extortion and crisis management costs (PR, IT Forensics, Credit Monitoring, Legal Costs etc.).

The standard AVN 48B War and Allied Perils exclusion clause excludes claims caused by, among others, any malicious act or act of sabotage. The malicious act or act of sabotage exclusion under AVN 48B directly responds to losses resulting from a cyber-attack as defined by the PRA. Under the English law, an insurer will only be liable for losses proximately caused by the peril covered by the policy. The proximate cause refers to the dominant, effective or operative cause of the loss.

There can be the case when, in aviation accidents, multiple proximate causes of a loss which operate concurrently can occur. The question which arises in this respect is whether an insurer will be liable in circumstances where not all the proximate causes of a loss relate to perils that an insurer is underwriting.

Therefore, there can be two answers: on the one hand, where there are two proximate causes of loss, one of which is specifically covered and the other is neither specifically covered nor excluded, the insurer will in principle be liable for the loss and, on the other hand, where there are two proximate causes of loss, one of which is specifically covered and the other is specifically excluded, the insurer can rely on the exclusion in relation to the entire loss.

If we were to take into account the scenario mentioned above, the supplier implanting a malware into a component later installed into an aircraft FMS computer and assuming that the malicious software would qualify as products defect and the aircraft manufacturer would be legally liable under product liability laws, the catalogue of exclusions would determine the scope of cover.

Having in mind that the provision of the policy does not cover

claims caused by any malicious act or act of sabotage, the exclusion of such acts is not limited to acts on board the aircraft. Notwithstanding that the implant of malware may qualify as malicious, the burden of proof is with the underwriters and it is high in cases where the perpetrators cannot be identified or it cannot be shown that this insured was targeted. If underwriters establish that the implant of malware qualifies as malicious and the insured was targeted, the claims may be excluded under the provisions of AVN 48B. These risks are subject to write back under the provisions of AVN 52 and separate sub-limits, are covered under the war covers and full policy limits will apply for TP losses either under the product liability insurance or the war excess liability policy.

As a concluding remark, it can be observed that the issue of cyber risk is one of the most systemic risks facing the insurance and reinsurance market. In order to provide effectiveness in adopting countermeasures, international efforts are essential to regulate cyber risks.

LO STATO DELL'ARTE NELLA RICERCA APPLICATA ALLA SICUREZZA AEREA IN EUROPA

Doriano Ricciutelli
Istruttore certificato dell´ENAC

Nel quadro delle attività incentrate sulla divulgazione dei lavori scientifici sinora eseguiti nell'Unione Europea, sotto l'egida della Direzione Generale (DG MOVE) della Commissione, il 14 marzo 2017 è stata pubblicata la quarta relazione di un'analisi tratta dal Transport Research & Innovation Portal (TRIP).

Si tratta del più vasto portale dedicato, giustappunto, alla ricerca e innovazione nel settore dei trasporti e riconosciuto unanimemente come uno strumento insostituibile di *know-how*, grazie alla disponibilità dell'ingente patrimonio informativo presente nel proprio database (circa 10.500 progetti e 400 programmi su scala nazionale, europea e internazionale).

Va preliminarmente detto che il rapporto di cui si discute, anche attraverso lo sfruttamento delle sinergie transnazionali incardinate nello spazio europeo della ricerca (ERA), offre una serie innumerevole di spunti di riflessione e un *humus* fecondo per approfondimenti tematici che alimentano il dibattito e la diffusione di proficui elementi conoscitivi in favore degli addetti ai lavori, degli stakeholder e dell'utenza in generale.

Emerge, poi, come reale valore aggiunto di tale compendio, la elaborazione d'una valutazione attenta degli aspetti tipici di security, raggruppati in sei macro aree e, segnatamente, quelle riferite alla "prevenzione e all'individuazione delle attuali minacce", alla "gestione della crisi", al fenomeno criminoso della "cybersecurity",

alla "formazione dello staff", alla "sicurezza delle merci" e alla "protezione dei passeggeri".

Ebbene, quanto al primo dei suesposti argomenti, la relazione si occupa dei progetti in buona parte inerenti alla realizzazione di dispositivi di monitoraggio e sorveglianza, a interfacce fisiche oltre che a precise soluzioni concretamente efficaci per pervenire ad una accettabile minimizzazione dei rischi afferenti al traffico aereo.

Del tutto plausibile appare, inoltre, la considerazione, testualmente riportata, secondo la quale l'*expertise* e i risultati della ricerca acclarati nel comparto avionico - oggetto in questa sede, ove meritevoli, di specifica attenzione - possano venir utilmente esportati, *mutatis mutandis*, verso le altre modalità di trasporto conformemente, invero, ad un *clichè* consolidato nell'*acquis* dell'Unione dopo i tragici eventi dell'11 settembre 2001.

In questo contesto vale la pena di menzionare il progetto "Flysec" (2015-2018) in grado di ottimizzare, attraverso procedure guidate e piuttosto snelle, gli sforzi esercitati da ACI (Airports Council Association) e da IATA (International Air Transport Association) e finalizzati al perfezionamento della security dei passeggeri dall'area landside all'airside e presso i varchi di imbarco loro dedicati. Dal punto di vista tecnico, "Flysec" raggiunge obiettivi ambiziosi integrando nuove tecnologie sulla videosorveglianza, l'elaborazione proattiva delle immagini a distanza nonché l'RFID (radio - frequency identification) per il tracciamento dei bagagli e la rapida gestione automatica dei bagagli. Al di là dei controlli di background più efficaci e del profilo di passeggeri, "Flysec" intende implementare un processo di sicurezza basata sui rischi, combinando le suddette tecnologie con l'analisi comportamentale e l'utilizzo di algoritmi cognitivi innovativi [(1)].

Muovendo lo sguardo alla materia di "crisis management" - per le cui fonti dispositive si rimanda all'Aviation Security Manual dell'ICAO, doc. 8973 e all'Annesso 17 della Convenzione di Chicago 10^ ed. in vigore dal 3 agosto 2017 - osserviamo che nel rapporto, oggetto di questo commento, sembra che gli stessi estensori conven -

(1) Si veda "Optimizing time to fly and enhancing airport security" (Horizon 2020), 5/2015 - 4/2018.

gano sull'affermato principio che, in situazioni emergenziali caratterizzate da un elevato grado di allarme di stampo terroristico, deve essere prioritariamente garantito un approccio che avvantaggi innanzitutto i progetti volti, *tout court*, al salvataggio delle persone e alla protezione delle merci.

In aggiunta, giova, qui, segnalare il sistema "TASS" ideato per la sorveglianza multilivello e le segnalazioni necessarie al monitoraggio della sicurezza aeroportuale, a sua volta ripartita in sei segmenti (ambiente, merci, persone, aerei, veicoli-flotta e impianti) controllati mediante diverse tecnologie che vengono sincronizzate e centralizzate per la condivisione, da parte di ciascun operatore, dei benefici prodotti e la garanzia, finalmente, di concepire un "ambiente" di security totale "*no breach*".

In merito alla sicurezza "cibernetica" non sorprende che la oramai stretta dipendenza del trasporto aereo - e non solo - alla funzionalità degli IT system impegni i progettisti in una *mission* protesa, da un lato, sul versante del rafforzamento della resilienza *cyber* (allestendo procedure di ristabilizzazione in conseguenza di attacchi informatici) e, dall'altro, sulla tutela della privacy, con particolare riferimento alla gestione dei dati e delle rispettive implicazioni immateriali e degli obblighi di trasparenza.

In relazione alle esigenze tipicamente legate alla difesa dell'aviazione civile, nel novero degli aspetti maggiormente analizzati per ridurre la vulnerabilità da aggressioni terroristiche, i progetti conclusi nell'ultimo periodo (2012-2017) hanno puntato ad ottenere un giusto equilibrio tra una sicurezza standard e i parametri accettabili di facilitazione aeroportuale incrementando, nel contempo, l'efficacia e l'efficienza del controllo sui passeggeri.

E' esemplare nella fattispecie l'obiettivo riposto in "XP-DITE" (*Accelerated checkpoint design integration test and evaluation project*), ovverosia l'intento di sviluppare un modello centrato sul passeggero tramite la progettazione di particolari ACP (airport checkpoint's) evoluti, insieme alla modifica di quelli esistenti, per affrontare adeguatamente le nuove sfide aperte alla security globale negli aeroporti, non disgiunta dall'introduzione di un insieme validato di protocolli, strumenti e fattori etici, che possono venir estesi anche ai trasporti di massa nonché ad altre analoghe applicazioni.

Si annoti, altresì, che che "XP-DITE", finanziato nell'ambito del 7° RTD Framework Programme, annovera, *inter alia*, risorse assai preziose in quanto associate alla adeguatezza di alcuni nuovi componenti di apparecchiature di screening per i futuri ACP già in avanzata fase di completamento, tra cui un meccanismo di rilevamento di esplosivi a raggi X, uno scanner di sicurezza e tecnologie di identificazione e di tracciamento biometriche.

Passando all'esame del capitolo attinente alla "formazione", ci accorgiamo agevolmente di un'ampia diversificazione dei target posti al centro delle numerose, relative progettualità che arricchiscono l'agenda TRIP; vale a dire che si spazia dalla focalizzazione sulla platea dei singoli fruitori (controllori, manager, impiegati di frontline nei terminal, etc) alle tipologie di training (basic, refresh, aggiornamento normativo, etc.), dallo studio delle innovazioni tecnologiche applicabili nei servizi di sicurezza all'interpretazione e alle correzioni dell'errore umano mediante l'uso di simulazioni *ad hoc* per la più idonea reazione alla minaccia.

E' appena il caso di menzionare il progetto "Benosa" formulato per lo sviluppo di un programma formativo destinato all'industria impegnata nella security aeroportuale e che coinvolge, altresì, un consorzio di utenti accademici, PMI e esperti del comparto con maturata esperienza anche in scienze sociali.

Si tratta in pratica della utilizzazione a fini didattici di un evoluto software capace di attivare simulazioni comprendenti l'individuazione e la previsione dei comportamenti riscontrabili in circostanze contingenti e "sotto stress", grazie ad osservazioni dirette e multisettoriali del comportamento di gruppo, contribuendo così ad eliminare in maniera significativa i rischi derivabili da "azioni ostili" contro il trasporto aereo.

Risulta, quindi, palese che le simulazioni incluse nel predetto software forniranno la piattaforma per i moduli ed i pacchetti di formazione da impiegare - peraltro a un costo minimo - negli aeroporti di tutta Europa.

Non si trascuri l'importanza anche di un progetto affine contraddistinto dall'acronimo "Bodega", rivolto a fornire - come autentico *leitmotiv* - progredite risposte d'ispirazione sociale e tecnologica -

mente all'avanguardia per arricchire le prestazioni professionali delle guardie di confine ottimizzando, in parallelo, la gestione armonizzata dell'attraversamento transfrontaliero dell'Unione, facente parte integrante della policy europea di Schengen e del relativo codice, ex regolamento UE/399/2016[(2)] .

A ben vedere il progetto si concentra sulla levatura del fattore umano, sulle proprietà degli equipaggiamenti e sui processi di verifica alle frontiere, non disgiungendosi da un accurato esame dei dati comportamentali dei viaggiatori allo scopo precipuo di sviluppare una "casella" di strumenti denominati "Proper", volti a migliorare gli attuali livelli di *performance* dal citato personale durante l'espletamento dei servizi.

Considerando ora il quarto dei nostri sopraindicati temi, si deve prendere atto che l'attuale organizzazione del "cargo" è orientata, *à juste titre*, al raggiungimento della piena conformità agli standard di massima efficienza e della velocizzazione delle spedizioni, caratteristiche queste che, per contro, rendono estremamente vulnerabile alle potenziali minacce la sicurezza del traporto aereo in un siffatto, delicato settore commerciale.

Ecco, allora, il richiamo al progetto "Citrimacc" (2015-2017), nel cui *core* risiede una "piattaforma intelligente e sicura" - per il carico dei container e lo scambio di informazioni - atta a ridurrei costi dello screening ed eliminare i rischi di manomissione coordinando materiali compositi, bloccaggi del codice PIN, atti di spedizione elettronici (e-freight), software web per dati "storage" e mezzi di comunicazione complementare ridondanti, basati su tecnologia GPS, GPRS (general packet radio service) e RFID per la visibilità continua in tempo reale.

Orbene, è il momento di citare il progetto "Fly-Bag 2" (2012-2015) che rappresenta il *follow-up* del precedente "Flybag", ideato per costruire nuovi contenitori per la cabina degli aeromobili necessari a stabilire l'ubicazione delle bombe cosiddette "a rischio minore" ed alla mitigazione degli effetti di un'esplosione a bordo, causata da materiali esplosivi celati nei bagagli caricati nelle merci.

(2) BordDerGuArd - proactive Enhancement of Human Performance in Border Control (Horizon 2020), 6/2015-05/2018).

Oltretutto, rileviamo per rilevanza ed analogia anche il progetto "Eurosky" (2013-2017) rivolto a introdurre misure di facilitazione per la salvaguardia delle catene di approvvigionamento internazionali del cargo, che appare in grado di affinare sia il rilevamento automatico - assieme alla risoluzione di allarmi riferibili a sostanze pericolose - che le capacità operative dell'infrastruttura tecnologica attrezzata a collegare elettronicamente tutte le parti ricomprese nella filiera della movimentazione di merci.

Sul punto va rammentato che la disciplina attinente alla sicurezza del cargo assume un particolare rilievo nella più recente normativa di settore dell'U.E. introdotta dal regolamento 815/2017/UE (da applicarsi dal 1 giugno 2017) che, in misura alquanto pregnante, ha inteso rivisitare il precedente regolamento 1998/2015/UE, nel panorama di un unico spazio aereo europeo ove siano garantiti i regolari flussi del commercio internazionali in totale sicurezza e conviene riconoscere che l'iniziativa di "Eurosky", in tale prospettiva, offre di certo una risposta sistemica di tutto rispetto.

In una simile ottica, nel corso della 93 ^ riunione del comitato AVSEC del 21 e 22 giugno 2017, la Commissione europea ha appunto fornito chiarimenti di dettaglio sulle modifiche apportate, *in subjecta materia*, dalla suindicata riforma con particolare enfasi all'"Air Cargo Database" e, nella circostanza, si è altresì discusso a proposito delle prossime strategie per le verifiche da effettuare sugli automezzi adibiti al trasporto merci aventi accesso in airside e sulla pertinente problematica tuttora aperta dell'"Integrated EU aviation security risk assessment on inbound flights".

Da ultimo non resta che affrontare la questione della "sicurezza dei passeggeri" e, al riguardo, il documento in parola si sofferma a delineare i caratteri del progetto "Consortis" (2014-2017), appositamente misurato per rilevare anomalie connesse alla presenza di articoli proibiti celati a bordo di velivoli, utilizzando una combinazione comprendente una videocamera da "submillimeter wave", un radar tridimensionale di *imaging* e un'ottica meccanica a scansione.

In seguito è richiamato un progetto simile al precedente noto come "Vulcan" (appartenente al 6° RTD Framework Programme) che si propone di approdare, attraverso l'attivazione di "test alle aero -

strutture (a scala)", su un piano di analisi mirata essenzialmente ai materiali compositi e ibridi, utilizzati per la fabbricazione di aerei e di poter, ergo, ridurre i danni potenziali provocati ai velivoli dagli effetti di esplosioni e d'incendi di natura intenzionale.

Alla luce delle suddette premesse, si può convintamente affermare che, atteso l'indiscusso *trend* emergente dalla capillare distribuzione e dal consistente numero dei progetti presentati in seno all'Unione Europea, la ricerca nel settore della sicurezza del trasporto aereo nell'ultimo periodo di riferimento, grazie anche ai cospicui finanziamenti erogati, amplia di gran lunga qualitativamente la propria sfera di intervento.

Infatti, se può ritenersi soddisfacente l'attuazione del Settimo Programma Quadro, successivamente, con le "Sfide delle Società Sicure in Horizon 2020" si è potuto imprimere, *soi disant*, un "definitivo" impulso per sfruttare appieno il potenziale della ricerca applicabile alla security.

Sul fronte dell'innovazione, in sintesi, non sono altrettanto mancati alcuni brillanti risultati soprattutto nella ideazione di tecnologie estremamente moderne per la prevenzione delle minacce (*ex multis*, apparati ottici di ultima generazione per il rilevamento *stand-off*, o per l'identificazione degli esplosivi in scenari reali a lunga distanza, o per l'individuazione delle posizioni di passeggeri sospetti, o per l'utilizzo di veicoli aerei senza pilota e di sensori per il monitoraggio delle aree critiche in aeroporto).

Concludendo la nostra breve esposizione, ci sembra doveroso auspicare che venga assunto dagli organi istituzionali preposti, nondimeno a livello nazionale, un impegno progettuale sempre vivo per esplorare ulteriormente nuove aree su cui imperniare la futura attività di ricerca e, tra queste, meritano un percorso privilegiato quelle involgenti la massimizzazione dei modelli di eccellenza per le configurazioni dei check-in nei terminal e, *last but not least*, quelle indirizzate alla protezione dagli attacchi informatici, considerati un *punctum dolens* alla stregua delle più recenti aggressioni di *cyber crime* verificatesi nei confronti di vettori e scali aerei europei [3].

(3) *e.g.* attacchi hacker del 27/5/2017 presso l'aeroporto di Kiev (Ukraina) Borispol e la probabile offensiva hacker del 27/5/2017 contro la compagnia aerea British Airways.

GLI USA VERSO UNA POLITICA UNILATERALE DELLE SANZIONI? IL CONGRESSO VARA IL CAATSA CONTRO RUSSIA, IRAN, COREA DEL NORD (E TRUMP)

Paolo Quercia
Direttore CENASS - Center for near Abroad Strategic Studies

Le sanzioni economiche e finanziarie sono uno degli strumenti a cui si fa maggiormente ricorso nei momenti di instabilità delle relazioni internazionali, quando il mondo è attraversato da tensioni che rimettono in discussione la gerarchia di potenza tra le nazioni ma il ricorso allo strumento militare non è una via praticabile.

Con le sanzioni, che molti vedono come l'alternativa liberale alla guerra (ma altri come lo straripamento della logica della guerra negli scambi commerciali), i Paesi sanzionanti cercano di coercere la volontà di uno Stato avversario o, molto più spesso, di punire una leadership straniera ritenuta incompatibile con i propri interessi e valori. Il più grande produttore di sanzioni sono gli Stati Uniti d'America, che vi fanno ricorso costantemente a partire dagli anni novanta.

Capi di Stato, ministri, giudici, oligarchi, imprese, banche, terroristi, aziende di stato operanti nei settori strategici dell'economia, narcotrafficanti, sono tutte categorie di soggetti che sono stati colpiti come destinatari di provvedimenti restrittivi o per la loro violazione. Negli USA le sanzioni economiche sono tradizionalmente state un campo riservato dell'azione di politica estera del presidente che, con pochi vincoli, aveva la facoltà di metterle e toglierle con un tratto di penna, firmando un Executive Order, rimuovendolo o applicando *executive waivers* a norme congressuali.

Da almeno vent'anni la politica estera americana fa un uso più o meno intenso dello strumento delle sanzioni economiche, che nei vari momenti storici ha assunto fisionomie differenti.

Il presidente Obama ha rilanciato lo strumento nell'ultimo decennio, facendovi ricorso in maniera particolarmente intensa con le sanzioni "*smart*", di nuova generazione, che cercano di essere sempre più specifiche e selettive, colpendo in particolare i gangli strategici di alcuni rapporti internazionali economici, banche ed assicurazioni in primis. Rilevante è stato l'utilizzo dello strumento sanzioni nel caso del braccio di ferro sul nucleare iraniano, che ha portato all'accordo sul JCPOA che ha consentito alla rimozione delle sanzioni secondarie americane.

Anche la reazione all'intervento russo in Ucraina del 2014 è stata affidata alle sanzioni economiche, applicate questa volta contro un'economia sviluppata ed integrata con l'Europa, soprattutto in campo energetico.

Le sanzioni selettive USA e UE contro Mosca - la più grande economia mai colpita dalle sanzioni americane sino ad oggi - rappresentano un nuovo inesplorato terreno.

Secondo alcuni esse sono una risposta giudicata come debole ed inadeguata, secondo altri un inutile ed inefficace costo per le aziende europee. Nella impasse è verosimile che resteranno in vigore a lungo sia quelle europee ed americane che le contro-sanzioni russe.

Ci si attendeva che l'avvento della presidenza avrebbe portato ad una revisione alle sanzioni contro Mosca, invece il passaggio all'amministrazione Trump si è svolto nel caos e all'insegna di profonde divisioni interne.

La nuova amministrazione, pur caratterizzata da una visione pro-business e filo russa, dopo un anno di presidenza appare aver perso il braccio di ferro con il Congresso che con una serie di iniziative parlamentari (ben quattro, poi confluite nel CAATSA) è riuscito ad imporre la sua linea di fermezza, riconfermando l'importanza delle sanzioni come veicolo principale di politica estera ma, cosa più importante, prendendosi sostanzialmente il controllo dello strumento ed esautorando il presidente.

Questo ci pare essere il senso della nuova legge quadro sulle sanzioni (*Countering American Adversaries Through Sanctions Act*, CAATSA) approvata durante l'estate in meno di una settimana dai due rami del Congresso USA con una schiacciante maggioranza (appena 5 voti contrari nelle due camere). A causa della vasta maggioranza, Trump non ha potuto non firmarla (il suo veto sarebbe stato battuto dalla sua stessa maggioranza di partito) nonostante egli appare essere manifestamente contrario alla Legge che amplia notevolmente le sanzioni contro la Russia, è penalizzante di molti interessi economici americani e lega le mani al Presidente, castrando la sua politica estera.

La parte più significativa dell'estensione delle sanzioni americane previste dal Titolo II del CAATS riguarda proprio la Russia e si prevedono sia misure primarie (rivolte cioè a soggetti giuridici americani o riconducibili al sistema USA) che misure secondarie (applicabili in teoria anche a soggetti giuridici europee).

Per quanto riguarda le misure primarie, rilevanti sono le misure sul finanziamento dei progetti nel settore energetico russo: vengono abbassati per i soggetti giuridici americani da 90 a 60 giorni i termini per la maturazione massima del debito per finanziamenti ad aziende russe *listed*.

Secondo una tendenza interpretativa di questa norma, rientrerebbero in tali divieti anche le fatture commerciali (*bills*) di beni e servizi saldate oltre il sessantesimo giorno dall'emissione; viene inoltre esteso anche al di fuori del territorio e delle acque territoriali russe il divieto per i soggetti giuridici americani di cedere beni, tecnologie e servizi in favore di progetti energetici che hanno più del 30% di partecipazione di società russe *listed*.

Queste sanzioni sono *mandatory*, ossia il presidente americano non può decidere se applicarle o meno ma vi è costretto. Le principali misure secondarie nel CAATSA prevedono sanzioni verso qualsiasi persona o soggetto giuridico che faccia investimenti nelle reti di trasporto del gas russo verso l'estero superiori al milione di dollari o superiori ad un tetto massimo complessivo annuale di 5 milioni di dollari. Queste sanzioni sono raccomandate e la loro applicazione resta a discrezione del presidente.

La nuova stagione delle sanzioni americane nell'era Trump si apre dunque in uno scenario confuso e complesso, che vede un apparente collasso dell'azione internazionale degli USA, una prevalenza della codificazione e del ruolo legislativo del parlamento e messo nell'angolo il principale attore della politica estera americana, l'unico in grado di negoziare i regimi sanzionatori con i suoi alleati europei.

La stagione della conflittualità economica globale che appare aprirsi dopo un anno di presidenza Trump rischia di assomigliare sempre più ad una guerra di tutti contro tutti, ma con una spiccata tendenza verso l'unilateralismo americano, sia per quanto riguarda la Russia che l'Iran. Su queste differenze rischia di ampliarsi il gap sull'uso strategico delle sanzioni tra UE e USA aggiungendo ulteriori incertezze per il mondo delle imprese a causa del possibile ampliamento del ricorso a misure secondarie.

Paolo Quercia. È stato analista del Centro Alti Studi Difesa dal 2001 al 2017 e ha lavorato come consulente per il Ministero del Commercio con l'Estero ed il Ministero degli Affari Esteri. È direttore del *Center for Near Abroad Strategic Studies* e Coordinatore del Comitato scientifico del progetto "*A World of Sanctions*" (AWOS) occupandosi di analisi di rischio paese nei regimi sanzionatori. www.paoloquercia.net

MARINE AVIATION & TRANSPORT
INSURANCE REVIEW

IN EVIDENZA

19' ANNUAL ASSICURAZIONI de IL SOLE 24 ORE
Milano, 6-7 novembre 2017
http://eventi.ilsole24ore.com/annual-assicurazioni-2017

Joint Cargo Committee Forum: Misappropriation
Londra, 15 novembre 2017 Old Library, Lloyd's
http://www.lmalloyds.com/LMA/Events/LMA___market_events/Joint_Cargo_Committee_forum_15Nov2017+E17134.aspx

European Shippers' Council Maritime Day 2017
Genova, 29 novembre 2017 - Palazzo san Giorgio
www.escmaritimeday.com

COMITATO DIRETTIVO

Andrea Dalle Vedove
Lars Lange
Anna Masutti
Pablo Mendes de Leon
Claudio Perrella
Neil Smith

HANNO COLLABORATO

Alberto Batini
Roland Kuesters
Paolo Lovatti
Paolo Quercia
Doriano Ricciutelli
Roger Sethsson

SEGRETERIA DI REDAZIONE
via Aldo Rossi, 4 - 20149 Milano
tel. 027764.290 - 027764.272
E-mail: matinsurancereview@ania.it

A CURA DI

Cristina Castellini
ANIA Direzione Generale Assicurazioni e Distribuzione
Dirigente responsabile Trasporti e Aeronautica