



Maritime Insurance against acts of terrorism

Alexandre de Soveral Martins
University of Coimbra – Law Faculty
soveralm@fd.uc.pt



1. Introduction

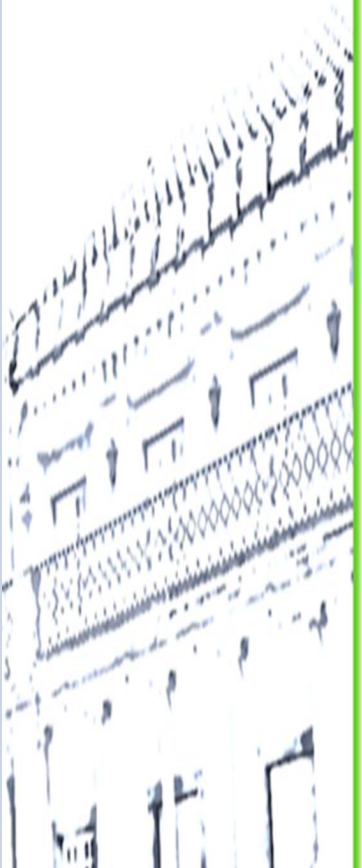
- Scarce information
- Massive damages
- Shipping, cruising and passenger ferries as targets
- Many alternatives available to perpetrate terrorist attacks (v.g. cyber attacks)
- High-risk zones, Areas of Perceived Enhanced Risk (APER)
- Navigation Warranties, Navigation Limits Clauses
- Usage Based Insurance (UBI)



- How to calculate risk, how to calculate actuarially correct premiums
- Baird Webel: «For the insurer to operate successfully and avoid bankruptcy, it is critical to accurately estimate the probability of a loss and the severity of that loss so that a sufficient premium can be charged»

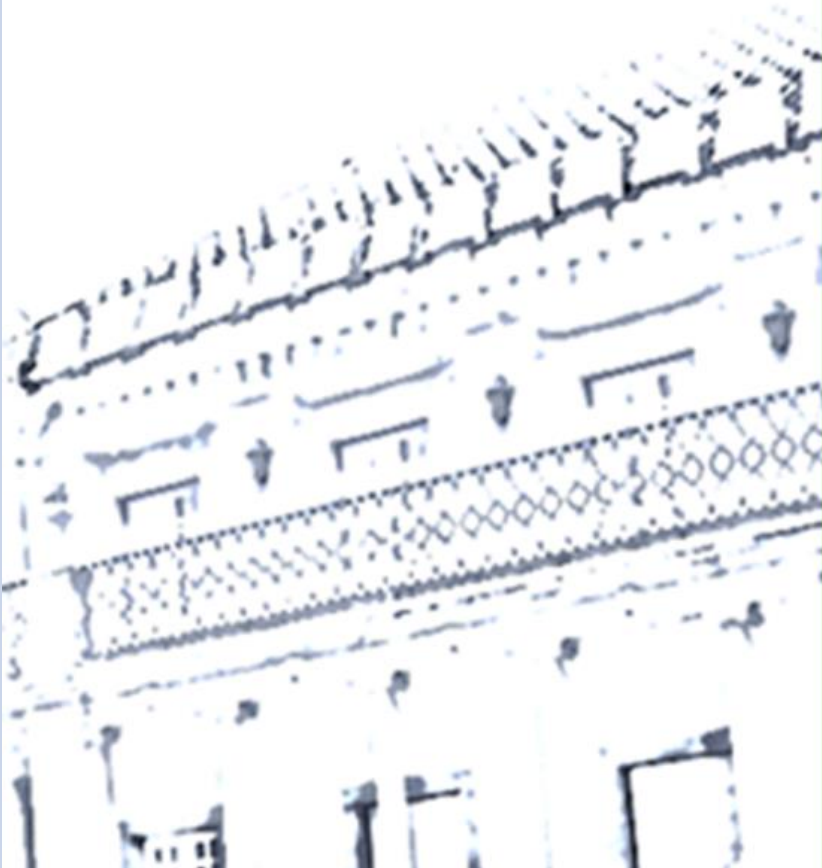
2. Shipping, Cruising, and the terrorist shadow. A definition

- Convention for the Prevention and Punishment of Terrorism (1937): «acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons, or a group of persons or the general public»
- Directive (EU) 2017/541 (Art. 3): list of acts committed with one of the following aims: «(a) seriously intimidating a population; (b) unduly compelling a government or an international organisation to perform or abstain from performing any act; (c) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation»
- International Cargo Clauses (Joint Cargo Committee of the Lloyd's Market Association) Termination of Transit Clause (Terrorism) 2009
- «an act of any person acting on behalf or, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of any government whether or not legally constituted or any person acting from a political, ideological or religious motive»



3. Marine insurance and terrorism. Some peculiarities

- The maritime industry environment. The supply chain
- Help from IoT and GIS (Geographical Information Systems)
- Looking for compensation: injured, owners, workers, mortgagor, mortgagee, shareholders, agents
- The liabilities:
 - terrorists and their organisations (?);
 - Ship owners or operators, employees;
 - Port operators and port authorities;
 - Security advisors



- 
- IMO. Guidelines on Maritime Cyber Risk Management
 - ISM (International Safety Management) Code
 - BIMCO, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, etc.: Guidelines on Cyber Security Onboard Ships
 - USA: NIST Framework (NIST – National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity)
 - ISO and International Electrotechnical Commission: 27001 Standard on information technologies
 - Port State Control and Cyber Risk Management
 - Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 «concerning measures for a high common level of security of network and information systems across the Union»; Proposal for DIRECTIVE repealing Directive (EU) 2016/1148 - COM(2020) 823 final 2020/0359 (COD)

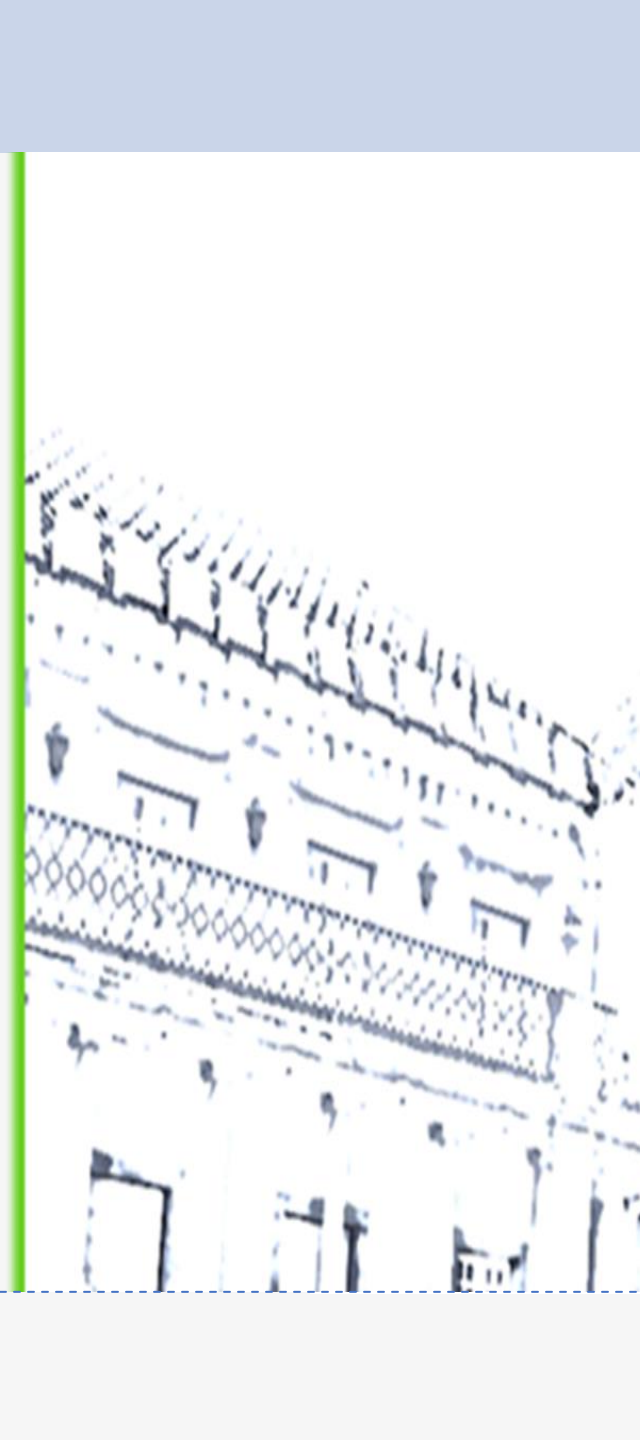


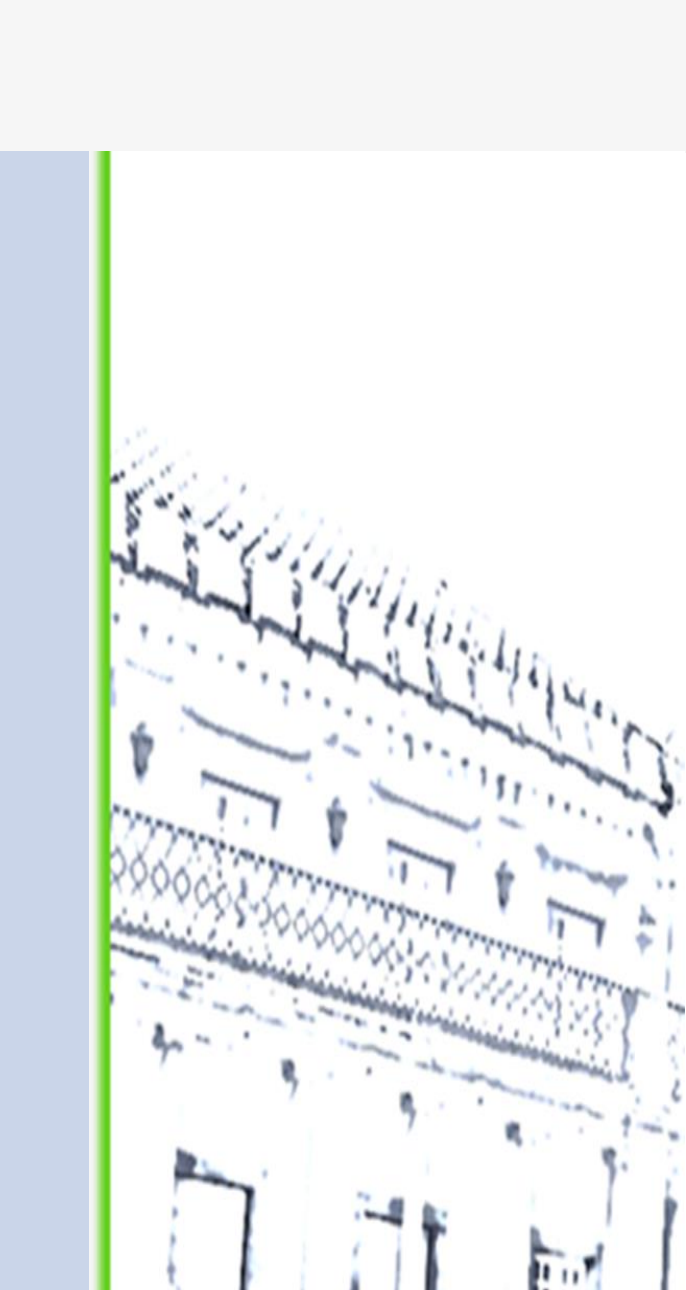
- Negligence
- Causation
- Evidence
- Occurrence and per occurrence limits of liability



4. Terrorism and Insurance. Availability

- Before 9/11
- After 9/11: exclusion clauses
- How to put the market back on track?
- USA: Terrorism Risk Insurance Act of 2002 (TRIA) and Terrorism Risk Insurance Program (TRIP)
- UK already had Pool Re: but marine policies not covered
- Russia, France, Spain, Australia, etc.
- Institute Cargo Clauses (A): excludes cover for loss, damage or expense «caused by any act of terrorism» (Clause 7.3.) or «caused by any person acting from a political, ideological or religious motive» (Clause 7.4).

- 
- Institute Strikes Clauses (Cargo): cover for loss or damage caused by «any act of terrorism» (Clause 1.2), and by «any person acting from a political, ideological or religious motive», although limited by the Transit Clause (Clause 5)
 - See also Institute War and Strikes Clauses (Clauses 1.5 and 1.6).
 - Cover for NCBR attacks is rare
 - Joint Cargo Committee Cyber Exclusion and Write-Back Clause (CL437), paramount
 - «1. In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to or arising from: 1.1. the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system; or 1.2. the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system [...]



Alternatives to try to make coverage available:

- a) Mandatory legal provisions imposing coverage;
- b) Public support (reimbursement) to insurance companies;
- c) Other economic incentives (tax...);
- d) Insurance pools, insurance funds;
- e) CAT Bonds;
- f) Co-insurance.

5. Preliminary conclusions

- Pools with insurance and reinsurance companies?
- But:
- National risks only?
- Exclusions of maritime insurance are frequent
- What about high seas? International Convention and Fund?
- Market inefficiencies and incentives to stay still

