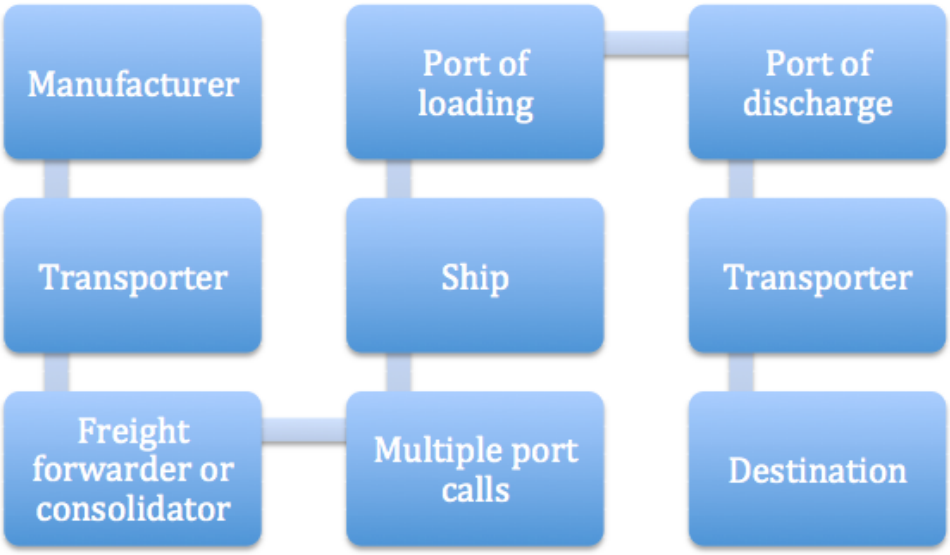
in the development of channels to gather and collate relevant information, detailed security plans, procedures related to the different security levels and implement these through the establishment of security related roles. What led to its creation is illustrated in its detailed set of recommended port and ship security measures aimed at minimising and discourage criminal acts and terrorist attacks (Ng and Vaggelas 2012, pp.677-78).

3.0. – Security in a transport environment

Historically, a port-state's efforts to create maritime transport policies were generally aimed at preventing marine pollution, improving safety standards and ensure efficient operation in every link of the supply chain (Ng and Vaggelas 2012, p. 674). However, after the 2001 terrorist attacks and other security incidents exposed the vulnerability of transportation systems the need for reform was recognised as a productivity component when two major port facility goals appeared to be related to security. (1) Respond to commercial needs and (2) provide a safe and secure harbour for operations and trade. Ports being the centring point of the logistics supply chain's many components are therefore crucial in the endeavour to safeguard the integrity of maritime transport systems. Thus, what used to be considered an overhead expense is currently a value-added business component that increases profits through mitigation of harm-associated costs (Christopher 2015, p.10).

Figure 1. **Supply-chain flow chart**



Source: Edgerton, 2013

governmental subsidy. Costs also arise from the undeniable fact that security installations use much-needed port space, limiting or restricting capacity and growth ((Ng and Vaggelas 2012, pp.690-91).

Table 1. **Operational results (1999-2005)**

Year	Container throughput (000' TEUs)	Cargo throughput (000' tonnes)	Total arrivals (Ocean and river vessels)	Average laytime (Ocean vessels)
1999	16 211	168 838	212 230	72h
2000	18 098	174 643	216 670	
2001	17 826	178 210	214 740	55,6h
2002	19 144	192 510	218 480	
2003	20 449	207 612	218 060	
2004	21 984	220 879	225 420	47h
2005	22 602	230 139	231 810	44,2h

Source: Mardep, 1999, 2001, 2004, 2005

A natural consequence of progressing technology and an increasingly well-educated workforce is improved performance in cost-reduction and efficiency. *Table 1* illustrates that there is no evidence to suggest that the implementation of such a comprehensive security regime has been a hindrance in the Ports endeavour to increase efficiency and maintaining operational competitiveness.

It should, at this point, be noted that the Port's application of the Code merely meets required standards with limited additional measures as facility operators wish to limit certain expenses. Though the Port has forgone biometric ID systems, seen in many American and some European ports, it possesses a complex legal and structural foundation that enforces the necessary measures with an undeniably accomplished performance (Ng and Vaggelas 2012, p.690). Much like The United States Security and Accountability for Every Port Act of 2006 and United States Maritime Transportation Security Act of 2002, the Code's primary aim is to deter and minimize terrorist attacks (Edgerton 2013, pp.17-18). After nearly 10 years of an unfailing L1 notification it was determined that further security enhancements beyond the initial