Università di Genova | DIEC DIPARTIMENTO DI ECONOMIA

INTERNATIONAL MARITIME AND TRANSPORT LAW COURSE MARITIME AND TRANSPORT LAW COLLOQUIUM

TRANSPORT LAW DE LEGE FERENDA 2021

Inter-university Centre - Dubrovnik, Croatia
6 -11 September 2021

NEW DEVELOPMENTS IN CYBERCRIME IN SHIPPING

GIOVANNI MARCHIAFAVA

Department of Economics, University of Genoa
gmarchiafava@economia.unige.it

Università di Genova | DIEC DIPARTIMENTO DI ECONOMIA

Thursday, 9 September 2021

SHIPPING AND SHIPBUILDING INDUSTRY - LEGAL ISSUES

SESSION I: RECENT DEVELOPMENTS IN SHIPPING LAW (09:00-11:45)

NEW DEVELOPMENTS IN CYBERCRIME IN SHIPPING

Giovanni Marchiafava

Department of Economics, University of Genoa
gmarchiafava@economia.unige.it

FINANCIAL TIMES
WORLD BUSINESS NEWSPAPER
TUESDAY 7 SEPTEMBER 2021
EUROPE

3.70

Flying low
Airlines' carbon offset prices are not high enough — INSIDE BUSINESS, PAGE 6

Shades of Mao
Does Xi's crackdown herald a second cultural revolution? — FT SERIES, PAGE 17

Working from jail
Using prisoners to fill labour gaps is a short-term fix — SARAH O'CONNOR, PAGE 19

Guinea coup
Aluminium at 10-year high

Residents of Conakry, Guinea's capital, cheer on soldiers yesterday after 83-year-old president Alpha Condé was overthrown in a military coup.

The junta has urged mining groups in the country to continue operations as he insisted that a unity government would be established. Guinea supplies a quarter of the world's bauxite, the main ingredient in aluminium, mostly to China and Russia. Aluminium's price hit the highest level in a decade yesterday.

Global powers have condemned the coup, with the US saying it "could limit the ability" of Guinea's international partners "to support the country".

Report page 2
Markets page 10
Lex page 20

Souleymane Camara/Reuters

Germany blames Russia for wave of cyber attacks in election run-up

Berlin cites 'phishing' emails • Protests passed to Moscow • Tight race to succeed Merkel

GUY CHAZAN — BERLIN

Germany has accused Russia of launching a spate of cyber attacks on politicians amid suspicions that Moscow is interfering in this month's election to decide who succeeds Angela Merkel.

The warning comes ahead of what appears to be the most open election in

passed Germany's protest directly to Vladimir Titov, Russia's deputy foreign minister, at a meeting of the two countries' security policy working group last week, Sasse said.

the pro-business Free Democrats on 12.5 per cent.

It is unclear which party Moscow would like to see win the election. Both Scholz and Armin Laschet, the CDU/CSU's candidate for chancellor, have struck emollient tones on Russia.

However, Annalena Baerbock, candi-

Germany has previously said

the BfV, said in July that foreign intelligence agencies saw the Bundestag election as a "significant target" and were exploring ways to affect the outcome.

Germany has long accused Moscow of seeking to access the digital networks of its political institutions. Merkel said last year that there was "hard evidence" that Russian forces were behind a huge hack

Briefing

Belarus activists handed 10-year terms
A court in Minsk sentenced two opposition activists to decade-long prison sentences for leading a protest movement against Alexander Lukashenko, who has been Belarus's president since 1994.— PAGE 2

Maersk cites cause of shipping crisis
One of the world's key port operators has warned that the shipping and supply-chain crisis that has left shelves empty on the high street can be resolved only by a slowdown in consumer demand.— PAGE 6

French cinema icon Belmondo dies
Jean-Paul Belmondo, the actor who made his name in Jean-Luc Godard's New Wave of cinema and became a beloved star of comedy and action films, has died at the age of 88.— PAGE 4

Taliban takes last area of resistance
The Taliban has declared victory over Afghanistan's last opposition stronghold after resistance fighters in Panjshir said an attack had inflicted big casualties on its leadership.— PAGE 4; NOTEBOOK & LETTERS, PAGE 18

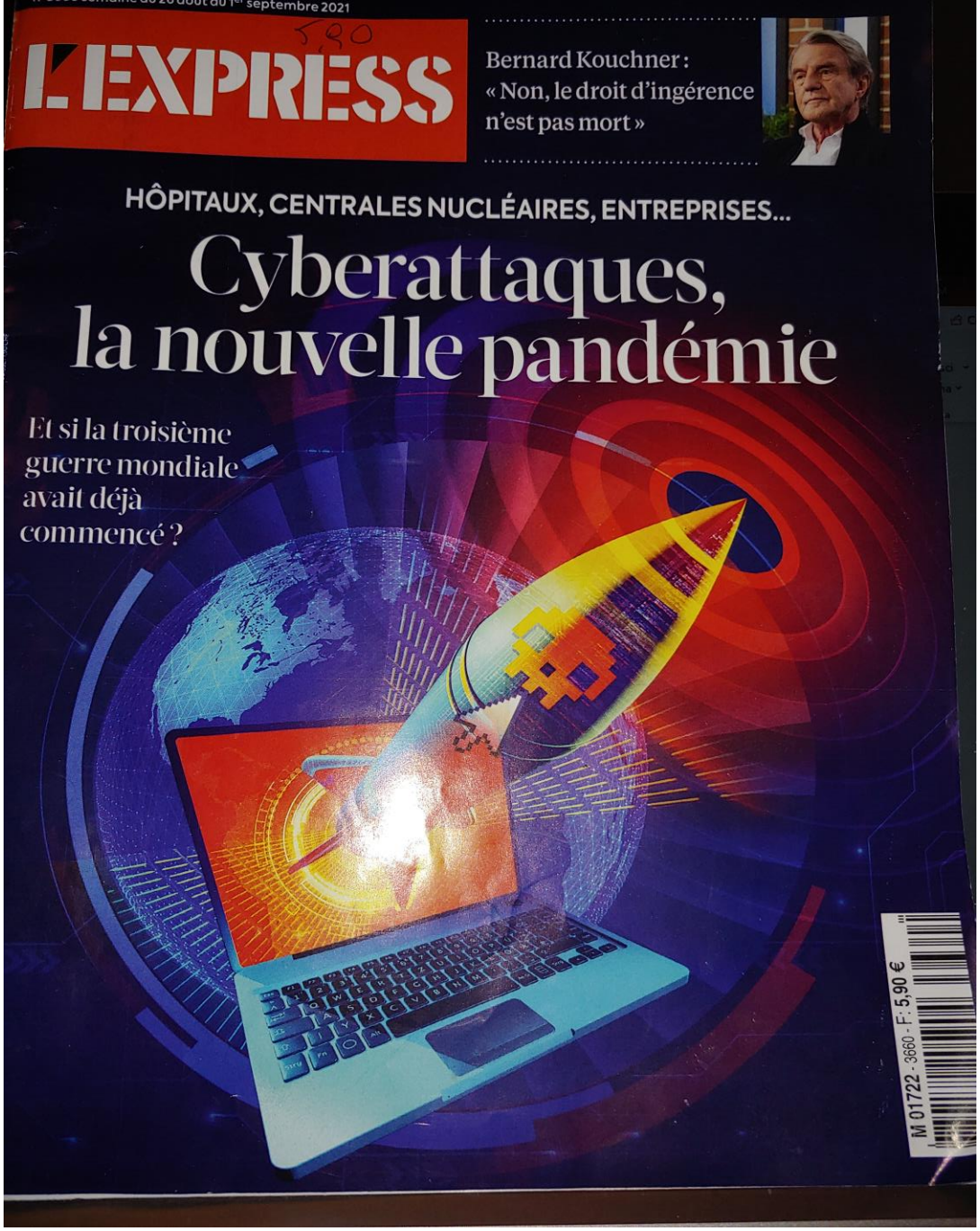
Indian stocks buoyed by foreign buying
A rally for Indian equities has put the country's market on course for its strongest performance since 2017, as foreign buying returned on signs of green shoots after rampant Covid-19 outbreaks.— PAGE 10

Cao Cao profits from pressure on Didi
Chinese state-owned funds are piling into Cao Cao, a rival to Didi, which is facing regulatory heat. Cao Cao said it had raised Rmb3.8bn ($588m) from a group of state-owned funds in the city of Suzhou.— PAGE 6

Iconic UK metals trading forum reopens
The LME reopened its iconic trading floor after an 18-month hiatus because of the pandemic, although questions remain about the long-term viability of Europe's largest open-outcry pit.— PAGE 9

Datawatch

Fewer suicides
Related deaths per 100,000 in England and Wales, April to June
10 to 24 · 25 to 44 · 45 to 64 · 75+


L'EXPRESS
Bernard Kouchner :
« Non, le droit d'ingérence
n'est pas mort »
HÔPITAUX, CENTRALES NUCLÉAIRES, ENTREPRISES...
Cyberattaques,
la nouvelle pandémie
Et si la troisième
guerre mondiale
avait déjà
commencé ?
M 01722 - 3660 - F: 5,90 €

Cybercrime: General Aspects

Definition

Cybercrime

- consists of criminal acts committed online by using electronic communications networks and information systems

- can be classified in three broad definitions:

1. crimes specific to the internet, such as attacks against information systems or phishing (fake bank websites to solicit passwords enabling access to victims' bank accounts)

2. online fraud and forgery (large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code)

3. illegal online content (child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia)

N.B. Key target for cybercriminals is not just financial data, but data more generally

Cybercrime: General Aspects

Cybercrime is:

- increasing very fast (acceleration in Transport > Digitalization + Autonomous Vehicles)

- becoming more aggressive and challenging

- assuming various forms of cybercrime, including high-tech crimes and data breaches

- growing problem for countries, such as EU Member States, in most of which IT infrastructures are well developed

Cybercrime: General Aspects

Economic Impact

- Cyber Attacks Cost in 2020 (McAfee): $ 1000 billions = 1.3% of the Gross Domestic Product (GDP) (*)

- - in 2019: $ 800 billions

- French Insurance Indemnity Cost in 2020: € 217 millions (*)

(*) Magazine L'Express no 3660/2021

- Cyber Attacks in Shipping Cost

e.g.,

In 2017 Maersk (integrated container logistics company) fell victim to a global cyber-attack which saw operations disrupted for more than two weeks, equipment having to be destroyed, and $ 300 million being spent to ensure recovery

Italian Cybercrime Case, 31 July/1 August 2021

Hackers had attacked and shut down the IT systems of the company that offered COVID-19 vaccination appointments for the Lazio Region through its website

Lazio Region
- manages by such systems services for 5.9 people living in a large area surrounding Rome
- is the second most populated region of Italy and includes the country's capital, Rome

This attack likely began after administrator credentials of an employee of the company that manages the computer network of the Lazio Region were compromised and obtained by the threat actors, thereby allowing the attackers to log on

This cyberattack was a
- ransomware attack
- significant attack for Italy because it targets a critical infrastructure of a large local public administration and involves a very large part (of the IT system)

Cybercrime: General Aspects

Ransomware cyberattacks are becoming increasingly sophisticated and more targeted

Number of targeted ransomware cases has increased over the past year, which has led to a
- significant increase in threat actor capability
- higher impact on victims

Ransomware attackers continue to target:

- public organizations
- - local governments and ministries
- - other public bodies
- - - hospitals
- - - universities, and high schools

- private organizations

- critical infrastructures (e.g., energy, transport)

Cybercrime: General Aspects

COVID-19 pandemic crisis

- COVID emergency has affected the cybercrime field

N.B. cyberattacks targeting energy, health, industry, transport, took place well before the crisis had a substantial effect in Europe and USA

- COVID-19 crisis was not a trigger for cyberattacks

- COVID emergency has increased of the attack surface, with unmanaged endpoints/devices (PC systems) being remotely connected and having access to companies' information technology (IT) infrastructure

N.B. Smart work/telework lead some companies to let down their guard with respect to cybersecurity (some of their IT security policies and some IT security responsibility has been transferred to the individual users, where varying levels of (or lack of) associated security training has created a new gap in security). This has subsequently provided new ways for cyber-actors to gain access to companies' IT infrastructure

International Cybercrime Rules

- **Budapest Convention 2001 on Cybercrime**

- adopted by the Council of Europe
- entered into force in 2004
- 66 Contracting States (Italy, Law 48/2008)

- **Budapest Convention 2001 on Cybercrime**

- is 1st international legal instrument on crimes committed by Internet and other computers networks > serves as guideline > not replace the national cybercrime rules

- regional character

- aims at harmonizing the domestic criminal substantive and procedural laws on Cybercrime
- - provides powers in domestic criminal procedural laws necessary for the investigation and prosecution of offences
- - introduces fast and effective regime of international co-operation
- - does not deal directly with Cybercrime in Shipping
- - some of the offences could be applicable to Cybercrime in Shipping (e.g., illegal access, illegal interception, data interference, system interference, misuse of devices)

International Cybercrime Rules

Budapest Convention 2001 on Cybercrime

Article 7

provides the introduction in their legal system criminal offences on "*the input, alteration, deletion or suppression of computer data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches*"

Article 7

- protects also measures adopted in shipping to guarantee the integrity of the electronic identification documents and readable transport document devices protected by cryptography techniques, and the passenger check systems

International Cybercrime in Shipping Rules

Issues on Cybercrime in Shipping issues

- Late Awareness about Cybercrime in Transport

- Lack of Wording /Glossary of Terms /Terminology (Updated) in Cybercrime in Shipping

- Lack of a Dedicated Cyber Security Governance in Shipping

- Lack of Coordination

International Cybercrime and Cybersecurity in Shipping Rules

- **NO, specific mandatory legal instruments in dealing with cybercrime in shipping**

= SOFT LAW

Legal initiatives are mainly the responsibility of each State
= NO LEGAL UNIFORMITY

SOFT LAW + NO LEGAL UNIFORMITY =
NO CYBER-SECURITY and NO CYBER-SAFETY IN SHIPPING

- **YES, legal instruments on cybersecurity in shipping**

Cybercrime and Cybersecurity
are two sides of the same coin

Legal instruments on cybersecurity in shipping

- - are not legally binding

- - - BIMCO Guidelines on cybersecurity for ships (Version 4, 2020)

- - - IMO Maritime Cyber Risk Management Guidelines (2017) - MSC-FAL.1/Circ.3 on Guidelines on maritime cyber risk management

International Cybersecurity in Shipping Rules

- IMO Maritime Cyber Risk Management Guidelines (5 July 2017)

- - represent a basis for understanding and managing the cyber risks

- - provide practical recommendations on maritime cyber risk management related to cyber security and cyber safety

- - support shipowners and maritime operators in undertaking activities

- - activate procedures to ensure safety and security on board of ships in accordance with the provisions established by the International Safety Management (ISM) Code and International Ship and Port Facility Security (ISPS) Code

- - specify a definition of cyber risk and cyber-threat

- - - "*maritime cyber risk* refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised"

- - - "*threats* are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat"

- - highlight the criteria to establish and reduce the risk

- - formulate emergency plan

- - identify critical aspects and potential targets of the cybercrime

International Cybersecurity in Shipping Rules

International Maritime Organization

- - adoption of a resolution MSC.428(98)

- - - encouraging the administrations to ensure that the cyber risks are duly considered in the safety management no later than the first annual verification of the company's Document of Compliance (DoC) after 1st JANUARY 2021

- - - requesting the content to be brought to the attention of the stakeholders

- - - inviting to circulate the guidelines in maritime sectors

- - implementation of the Cyber Risk Management through other national guidelines and standards established by private and public bodies as:

- - - BIMCO Cyber Security Onboard Ships

- - - ISO/IEC 27001 (Standard in Information technology, Security techniques, Information security management systems, ISO Requirements)

European Union Cybersecurity Policy

EU Action on Cybersecurity - 16 December 2020

EU Commission and High Representative of the European Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy

THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

(JOIN(2020) 18 final)

Cybersecurity is a one of the EU Commission's priorities to face the coronavirus crisis (Recovery Plan for Europe; Research and Innovation Projects)

European Union Cybersecurity Policy

EU Cybersecurity Strategy

- covers the security of essential services as transport

- focuses on building a capability to respond to major cyberattacks

- aims at guaranteeing international security and stability in cyberspace

European Union Cybersecurity Policy

EU Cybersecurity Strategy

- Necessity to create strong national government bodies to supervise cybersecurity and share information with EU Member States = GOVERNANCE SYSTEM

- - NIS Directive: creation and cooperation of these bodies

- - Joint Cyber Unit (Proposal – EU Commission Recommendation 23 June 2021)

- - platform to ensure an EU coordinated response to cyberattacks and crises and give assistance in recovering form such attacks

European Union Cybersecurity Policy

EU Cybersecurity Strategy

Transport

EU Commission

- added provisions on cybersecurity to the EU legislation on aviation security

- will continue its efforts to enhance cyber resilience across all transport modes

Air Transport Cybersecurity

- **Commission Implementing Regulation (EU) 2019/1583 amending implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures**

- Main Objective of the Reg. (EC) no 300/2008 on common rules in the field of civil aviation security:

- - provide the basis of a common interpretation of Annex 17 (Security Annex) of the Convention on International Civil Aviation of 7 December 1944

- - setting common rules and basic standards on aviation security and mechanisms for monitoring compliance

- Amendment 16 to Annex 17 (Security Annex)

- - includes new and revised provisions on information-sharing, measures relating to passengers and cabin baggage, measures relating to cargo, mail and other goods, and cyber threats.

- - introduces new standards under chapter 3.1.4. related to national organization and appropriate authority and 4.9.1 related to preventive cyber security measures

Air Transport Cybersecurity

Commission Implementing Regulation (EU) 2019/1583 – ANNEX

Identification and Protection of Civil Aviation Critical Information and Communication Technology Systems and Data From Cyber Threats

- detailed measures to protect IT systems and data must be identified, developed and implemented

- national authority/agency competent to coordinate and monitor cyber-related provisions of Reg. (EU) 2019/1583

- standard background check for the personnel (security controls, air cargo access and mail, supplies requiring security control, critical information and communication technology and data access)

- **required skills and aptitudes for the mentioned personnel**

European Union Cybersecurity Policy

European Cybersecurity Competence Centre (ECCC)

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

ECCC is new European framework to support innovation and industrial policy in cybersecurity

ECCC and the Network of National Coordination Centres (NCCs) will

- strengthen the capacities of the EU cybersecurity technology

- protect EU economy and society from cyberattacks

- maintain research excellence

- reinforce the competitiveness of EU industry in this field

European Union Cybersecurity Policy

European Cybercrime Centre (EC3) set up by Europol (2013)

- strengthen the law enforcement response to cybercrime in the EU

- help protect European citizens, businesses, and governments from online crime

- **publication of the Internet Organised Crime Threat Assessment (IOCTA), a report on key findings and emerging threats and developments in cybercrime**

Italian Cybercrime in Shipping Rules

NO, specific rules on cybercrime in shipping

YES, general rules on cybercrime

- Italian Criminal Code (ICC - Codice penale)

e.g.

- - Article 615-*ter* ICC, Illegal Access to Computer System

- - Article 635-*bis* ICC, Damaging of computer information, data and programmes

- - Article 635-*ter* ICC, Damaging computer information, data and programmes used by the State or any other public body or a body anyway having a public utility

- - Article 635-*quarter* ICC, Damaging computer or telematic systems

- - Article 635-*quinquies* ICC, Damaging computer systems or telematic systems of public utility

- - Article 640-*ter* ICC, Computer Fraud

- Laws/Rules for specific cybercrime offences

Italian Cybersecurity Agency

Italian Cyber Security Agency

Decree 14 June 2021 no 82, Urgent Provisions on Cyber Security, Definition of National Cybersecurity Architecture, and Institution of National Cybersecurity Agency

Reasons:

Vulnerability of networks, information systems, digital services, private and public electronic communication can be exploited to produce a partial or total malware or interruption of

- essential functions and services to ensure civil, social, and economic activities which are vital for

- - State interest

- - public utility services with potential serious effects for citizens, companies, and public administrations to a such a degree to that national security can be jeopardized

Italian Cybersecurity Agency

Italian Cyber Security Agency

- operates under the responsibility of the Italian President of the Council of Ministers

- - Italian Interministerial Committee for Cybersecurity

- controlled by the Italian Interministerial Committee for the Security of the Republic

- is the Italian National Coordination Centre that will interface with the European Cybersecurity Competence Centre (ECCC) according to the European Union Law

N.B. The Ministry of Sustainable Infrastructures and Mobility (former Ministry of Infrastructures and Transport) is the Authority for the Transport Sector and Air, Rail, Road and Sea Subsectors

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

- **Circular no 24/2019**

Objectives:

- improve the staff training in maritime security and cyber risk awarness

- inform users on the availability of online training related to «Awarness in Maritime Cybersecurity»

Training and updating are essential aspects for staff preparation and growth

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

- **CIRCULAR NO 24/2019**

Addressees:

- **Harbour Office Staff (FSI, Port State Control Officer, Duly Autorised Officer).**

- The deadline to obtain the module's certificate: 31 march 2020

Notice to Shipping Companies, Port Authorities and Stackeholders (Master, Crew, Shipping Company Staff, Port and Port Infrastructures Staff, Technical Nautical Services Staff and Crew)

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

- **CIRCULAR NO 24/2019**

Module: Awareness in Maritime Cybersecurity

- designated to raise awarness in maritime security

- - provides necessary information and regulation to approach cyber security and the relevant legal issues in maritime sector

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

- **Circular no 155/2019**

IMO GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

- General Recommendations

- Identification Sistem's Vulnerabilities (information and operational technology)

- New Objective: Information and data protection

Vulnerability Assessment: Comparison of System Design, Integration and Maintanance (to define possible gaps and mistakes on the so-called cyberdiscipline)

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

Circular no 155/2019

Cyber Risk Management «[…]» should be defined by a comprehensive monitoring of the current organization, the desired organization and the results of the cyber risk management

Disclosure of gaps which should be assessed to reach the objectives of the risk management also by a risk prioritization

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

- **Circular no 155/2019, Re: Cyber risk management**

(Previous Circulars: Circular titled Security no 35/2017 - Circular no 8/2018

<u>It is considered necessary the adoption of a risk management framework by the companies</u>

Risk management framework must duly take into consideration the elements provided by the:

- Annex of Circular no 155/2019

- IMO Resolution MSC.428(98)

- MSC-FAL.1/Circ.3

- Provisions established by the NIS Authority for the companies which have been classified as Essential Service Operators (ESO)

Italian Cybersecurity in Shipping Rules

Italian Ministry of Infrastructures and Transport - Italian General Command of the Harbour Offices

ANNEX of Circular no 155/2019, Re: Cyber risk management

AIMS

- Identification of the ISM process related to cyber security

- Assistance to management companies in elaborating the «risk assessment»

- Protection of systems and information from the cyber threats

EFFECTS

- guarantee a safe ship management

- environment protection

crew protection

UniGe

DIEC