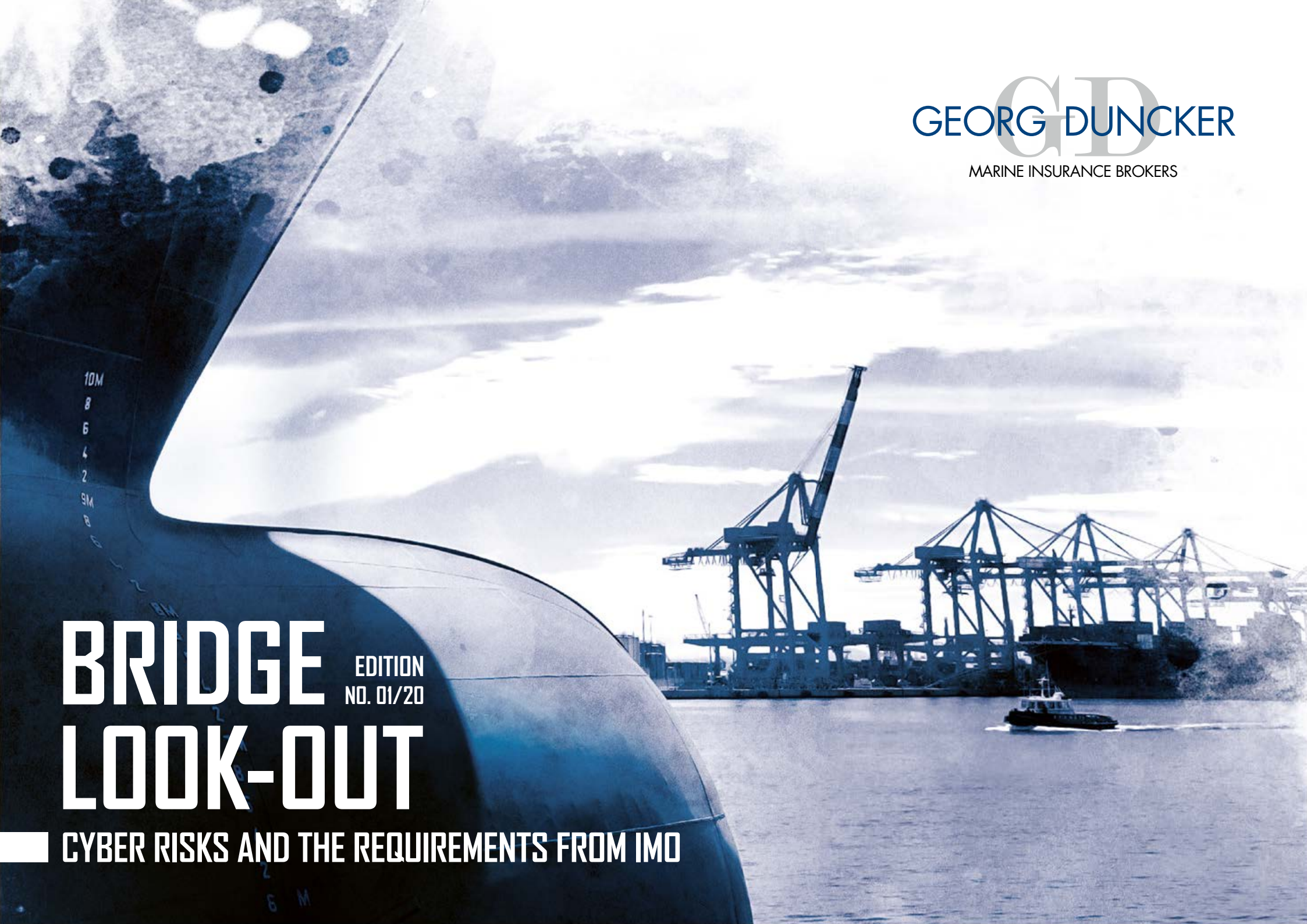


GEORG DUNCKER

MARINE INSURANCE BROKERS

BRIDGE LOOK-OUT

EDITION NO. 01/20

CYBER RISKS AND THE REQUIREMENTS FROM IMO

CYBER RISKS AND THE REQUIREMENTS FROM IMO

We are seeing an increase in the number of insurance related inquiries from Shipmanagers to cover cyber related risks for their vessels, as well as offices and other on-shore entities. Managers are often motivated by the IMO dated 16th of June 2017 resolution MSC.428(98)) which stipulates that Shipmanagers – or more precisely the DOC holder – have to incorporate the handling of cyber risks into the approved Safety Management System (SMS). Implementation has to be made latest by 1st of January 2021 and it founds its justification in the increased connectivity of the ocean going vessels and the consequential growing threat of attacks against vessels and their equipment.

An example of such a risk would be a vessel equipped with an Electronic Chart Display and Information System (ECDIS) without a paper navigational chart on board. The vessel could run into serious trouble if the chart system were to be infected by a virus.

It is important to be aware that in the majority of cases, neither the expenses incurred for the respective troubleshooting nor the costs for a potential delay are recoverable from Hull and Machinery (H&M) or Loss of Hire (LoH) insurers, or war risk insurers which otherwise would cover malicious acts. This is due to the fact that cyber risks are explicitly excluded under the regular H&M and LoH coverages. Nevertheless, this does not necessarily mean that such risks are not insurable. For example, several hull underwriters offer different products such as “buy back options” for cyber related risks.

Before deciding on a cyber insurance cover, Shipmanagers should seek further information on the products as they differ creating several hurdles of which Shipmanagers should be aware of. For instance, some products miss out insurance protection for War or LoH. Furthermore, it would be sensible to check the total sums recoverable and to the total insured limits under an underwriters’ overall portfolio. If an Underwriter were to be exposed to several extensive cases simultaneously, it may be that the total insured amount for all clients is exceeded and thus an apportioned reimbursement would place. This is more a theoretical situation, where cyber-attacks would have to increase on a massive scale; it is however a very realistic scenario and it is recommended that Shipmanagers bear this in mind.

Roughly speaking, one could split the various products into three types: one product from the Scandinavian market, which is simply a buy back option for the risks excluded under H&M, LoH or War coverage. Another product from the German market, based on the German conditions for H&M related incidents. And finally a product from the United States in cooperation with Lloyds, with a named peril coverage for H&M, War and subsidiaries. We at Georg Duncker would be more than willing to support and assist you in assessing potential cyber related coverages.

It is important to consider that not only vessels are at risk of being targeted, but the owning companies’ on shore entities face a number of different types of cyber-attacks. These can range from simple phishing emails, to hacking of internal email servers with fraudulent intent to intercept secret information, to interfering in transactions and transfers of payments. Cyber criminals are also capable of blocking the working process through infiltration of the company server in order to press for a ransom. The latest attack known as the “NotPetya” was a trojan-ransom-software which caused serious troubles at several corporations, amongst others to the Terminal administration of Maersk A/S and Deutsche Bahn.

In summary, we see several major reasons for Shipmanagers to consider covering against cyber risks. Such cover may be of assistance when implementing Owners’ or Shipmanagers’ SMS and the respective appropriate safety measures. Additionally, Shipowners and Shipmanagers may be requested to act prudently and proactively in order to guarantee the best protection of their shareholders’ interests and in turn, their own, thus avoiding any loopholes in the event of a cyber-attack.

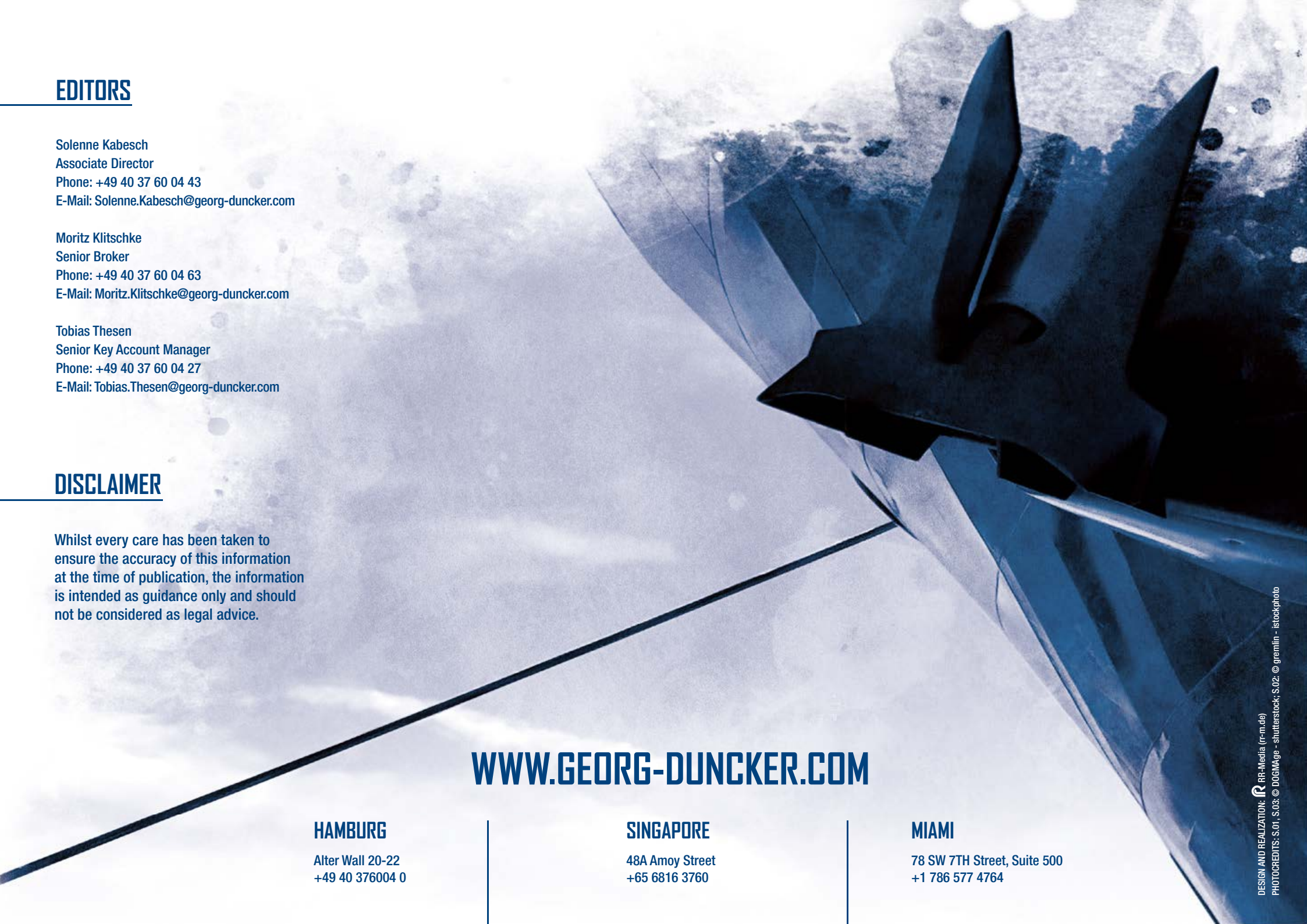
EDITORS

Solenne Kabesch
Associate Director
Phone: +49 40 37 60 04 43
E-Mail: Solenne.Kabesch@georg-duncker.com

Moritz Klitschke
Senior Broker
Phone: +49 40 37 60 04 63
E-Mail: Moritz.Klitschke@georg-duncker.com

Tobias Thesen
Senior Key Account Manager
Phone: +49 40 37 60 04 27
E-Mail: Tobias.Thesen@georg-duncker.com

DISCLAIMER



WWW.GEORG-DUNCKER.COM

HAMBURG
Alter Wall 20-22
+49 40 376004 0

SINGAPORE
48A Amoy Street
+65 6816 3760

MIAMI
78 SW 7TH Street, Suite 500
+1 786 577 4764

DESIGN AND REALIZATION: RR-Media (rr-m.de)
PHOTOCREDITS: S.01, S.03: © DOGMAge - shutterstock; S.02: © gremlin - istockphoto