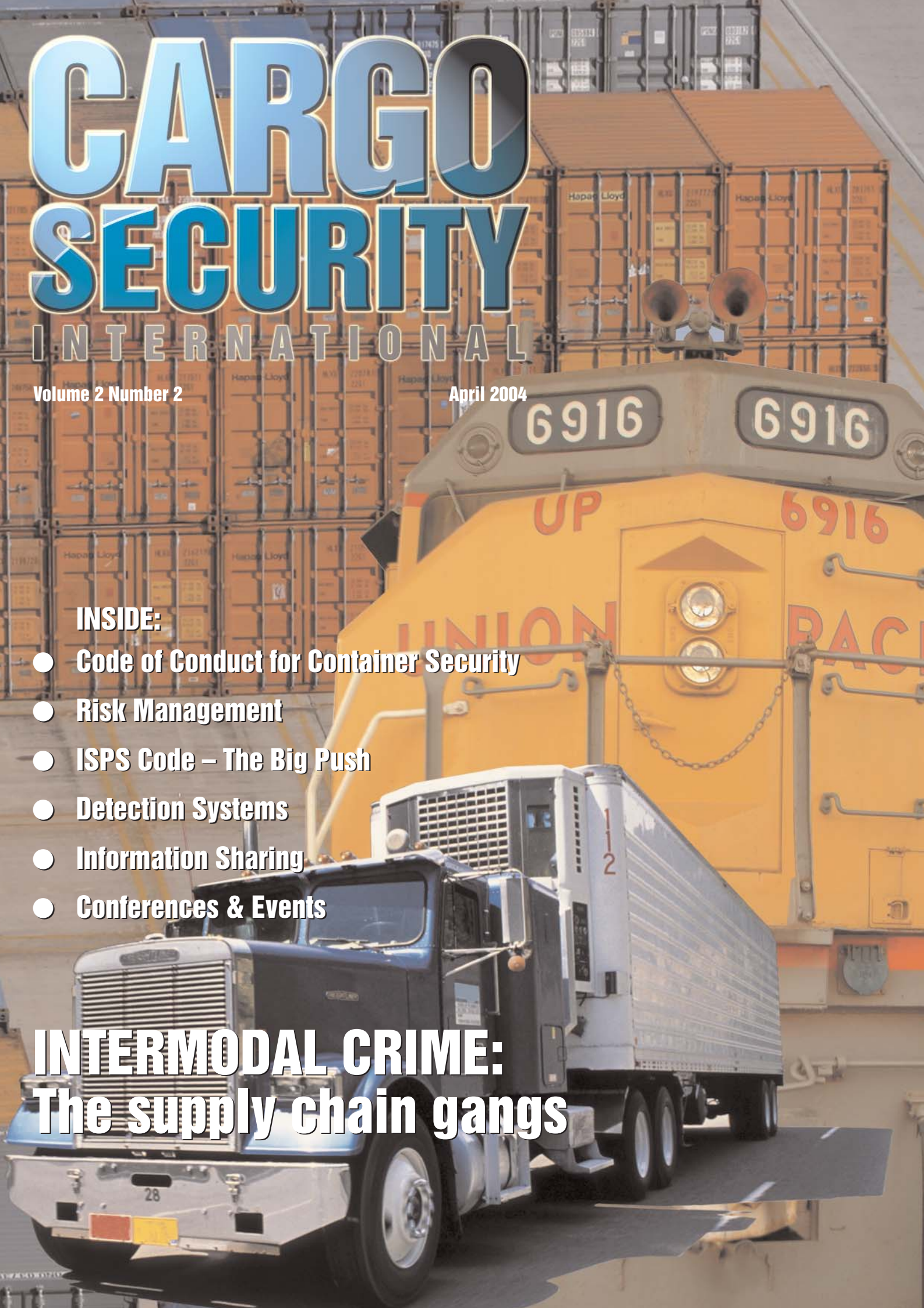
CARGO SECURITY INTERNATIONAL

Volume 2 Number 2 April 2004



INSIDE:

- Code of Conduct for Container Security
- Risk Management
- ISPS Code – The Big Push
- Detection Systems
- Information Sharing
- Conferences & Events

INTERMODAL CRIME: The supply chain gangs

It's good to share

Sharing information and threat analysis with ship operators and ports is a fundamental defence against future terrorist attacks, writes Kenneth Bergquist of the Maritime Information Sharing and Analysis Center and Kim Petersen, Executive Director of the Maritime Security Council

Kenneth P. Bergquist is the Executive Director of the Maritime Information Sharing & Analysis Center, Inc. He is the former US Assistant Secretary of the Navy and Associate Coordinator for Counterterrorism at the US State Department. He is also a retired Brigadier General in the Army's Special Forces and the first President of the US Joint Special Operations University.

Kim E. Petersen is the Executive Director of the Maritime Security Council and is the former Director for Security for Princess Cruises and Renaissance Cruises. Previously, he held senior staff positions with former US Secretaries of State Henry A. Kissinger and Alexander M. Haig and in both the US Senate and US Defense Department in the areas of national security and intelligence. Petersen is a former Captain in the US Special Forces.

The master of the tanker *Limburg* looked out on the placid waters of the Gulf of Aden and contemplated an uneventful arrival in port in the next few hours. Of course, he knew the history of the region, and in particular the horrendous suicide attack by al Qaeda on the *USS Cole* the previous year. But, that was an attack on the United States and its military. His company received no information that even hinted at the potential for similar attacks against merchant vessels. And, after all, the *Limburg* was French flagged and Belgian owned – why should it be a target?

As the ship slowed to pick up the pilot for entry into Aden, the bridge watch spied a small boat with two occupants approaching from the North. Not believing it necessary to take any evasive action, the Captain of the *Limburg* continued with his preparations to bring aboard the port pilot. Some minutes later, the tanker would shudder from a massive explosion amidships. The unthinkable had happened and the results were devastating: one crew member killed, 90,000 barrels of oil released into the ocean, and the ship seriously damaged. Only later was it learned that other ships visiting Aden had received information that indicated that just such an attack on merchant shipping was considered likely.

The failure to share information obtained by other shippers in the case of the *Limburg* was not anomalous. The sad truth is that timely maritime security and threat information has historically been denied to the very people most in need of it – the shipping and port communities. What little information governments were willing to provide was usually slow in coming and denuded of meaningful detail.

Far from a conspiracy of silence, the problem has always centered around two issues:

- the understandable desire of governments to classify information collected even from commercial sources and then limiting dissemination to those within government with a 'need to know'; and
- a lack of any one organization dedicated to processing, analyzing, and disseminating information available from one or more sources in the maritime commercial sector to those in the remainder of the sector who may benefit from such dissemination.

One consequence of the terror attacks of 9/11 has been a re-evaluation of information sharing with and within the maritime industry. For example, it has been revealed that Abd al Rahim al-Nashiri, who was al Qaeda's director of operations in the Gulf region, had masterminded the *Limburg* attack. Unprecedented details have been released, such as important new information about a series of devastating attacks al-Nashiri planned to orchestrate against US and Western shipping in the Mideast Gulf and Red Sea. According to official sources, those plots included plans to fly hijacked aircraft into US and coalition warships and attack commercial shipping with explosive-laden, suicide boats.

How then do we ensure that maritime security-related information gets from those industry sources who acquire the information to those such as the Master of the *Limburg*? Perhaps the most important source for maritime threat and security information is the soon-to-be-operating **Maritime Information Sharing & Analysis Center (M-ISAC)**.

Based in Ft. Lauderdale, Florida, with a collection and analysis node in Washington, D.C., the M-ISAC is being created to provide the partnership between the US Government and the maritime industry needed to share critical information regarding the security of maritime commerce. In 2002, **US Coast Guard (USCG)** officers inside the **US Department of Transportation**, Office of Intelligence and Security, approached the **Maritime Security**

'The M-ISAC is intended not only to serve the interests of US ports and ships, but also the over 60,000 foreign flagged ships, 20,000 overseas seaports, and the more than 250,000 crew and port employees around the world as well'

Council (MSC), a trade association specializing in maritime security issues, with the suggestion that the MSC sponsor the creation of an Information Sharing and Analysis Center (ISAC) for the maritime industry.

Other critical infrastructure ISACs already exist in the US, including surface transportation, airlines, financial services, and even railroads. Surprisingly, the maritime sector had been overlooked, probably because of the daunting nature of the industry it would serve. For example, the United States' maritime borders include 95,000 miles of open shoreline, 361 ports, and an Exclusive Economic Zone that spans 3.5 million square miles of ocean.

The US relies on ocean transportation for no less than 85% of goods consumed or produced. Each year, more than 7,500 commercial vessels make almost 51,000 port calls, with over six million loaded containers entering US ports, and growth predictions indicate that container cargo will quadruple in the next 20 years.

Prior to 11 September 2001, the primary focus of intermodal transportation was the safe movement of containers in a timely manner. As a consequence of the new terrorism threat realities, the US Government recognises that it must enhance existing security measures, introduce new technologies, and do a better job of cooperating with the maritime industry. The ultimate objective is to ensure the dissemination of critical threat and security information, so as to minimize the risks and consequences of a terrorist attack without appreciably affecting the speed and efficiency of maritime commerce.

However, the M-ISAC is intended not only to serve the interests of US ports and ships, but also the over 60,000 foreign flagged ships, 20,000 overseas seaports, and the more than 250,000 crew and port employees around the world as well. A massive – and disparate – constituency, to say the least.

What is an ISAC?

In May 1998, US President Clinton signed Presidential Decision Directive-63 (PDD-63) which recognized that unique public-private partnerships would be required to reduce critical infrastructure vulnerabilities in the US. Accordingly, PDD-63 mandated that departments and agencies of the Federal Government 'effect a closely coordinated effort of both government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative.'

In addition, PDD-63 declared: 'The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.'

PDD-63 also mandated that the Federal Government should 'consult with owners and operators of critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center' for each critical infrastructure industry sector. Such centers are intended to 'serve as a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and government'.

Elements of the Maritime ISAC

Upon accepting the challenge of the US Government, the MSC set out to create the foundation upon which the M-ISAC is being built. As the first member and sponsor of the M-ISAC, the MSC began the enormous task of meeting with and educating legislators and agency officials on the importance of an industry-controlled information sharing apparatus that would collect, analyze, and

'The sad truth is that timely maritime security and threat information has historically been denied to the very people most in need of it – the shipping and port communities'

disseminate industry-centric threat and security information. Funding for the M-ISAC has been a significant challenge, with over US$3 million required not only to purchase the IT infrastructure necessary but to support the global collection, analysis and dissemination requirements.

The aggressive protection of maritime infrastructure in the US will begin with information freely provided by M-ISAC members who have the capacity to collect information world wide. Utilizing member reports from ships and ports around the world, as well as collecting information from government and open sources, will permit the M-ISAC to undertake analysis and timely dissemination of threat information to those ships and ports at risk. This synergy of collection efforts will not come to pass without the whole-hearted support of the maritime industry for 'their' M-ISAC. The industry must be the owner and operator of the M-ISAC to ensure that the Federal Government's regulatory enforcement responsibilities do not discourage the willingness of M-ISAC members to report all relevant information, even information that would otherwise bring sanctions to the member were it reported directly to the Federal Government.

Recognising this reality, the **Department of Homeland Security (DHS)**, which now includes the USCG, the **US Bureau of Customs and Border Protection (CBP)**, and the **Office of Information Assurance and Infrastructure Protection**, has been working with the MSC to ready the M-ISAC for development of an initial operating capability during the second half of 2004. Collection of information from industry sources will be conducted in such manner as to preclude the identification of an industry source where such disclosure may bring about government sanctions for that reporting source.

The M-ISAC has been established as a not-for-profit corporation and has initiated the planning necessary to achieve initial operating capability. With the MSC as its sponsor, the M-ISAC will soon be soliciting membership from all industry associations, individual port authorities, shipping companies, international flag registries, recognized security organizations, and international classification societies. The maritime industry will own, manage and operate the M-ISAC with the mission of achieving a full partnership with the US Government concerning the timely and efficient exchange of maritime, security-related information based upon negotiated information exchange protocols.

Next steps

Once the operating agreement between the DHS and the M-ISAC is finalised, information sharing protocols will be developed and at least a limited functioning will commence. Congressional funding for the first three years of operations of the M-ISAC is being sought for Fiscal Years 2005-2007. Thereafter, continuing operations of the M-ISAC will be equally shared by the maritime industry and the US Government. Given that it will probably take three years to build up the membership of the M-ISAC, Federal funding for that brief period of time will demonstrate the commitment of the US Government to the establishment of the M-ISAC and to its partnership with the international maritime industry.

Protocols for information sharing will be developed by maritime industry representatives in conjunction with the various operating elements of the DHS. Membership by maritime commercial companies and industry associations in the M-ISAC will be entirely voluntary.

However, membership will offer maritime trade associations, shippers and ports the opportunity to receive analyzed security-related information from other industry members and to directly influence the relationship of the maritime industry with the USCG, the CBP and the Office for Information Assurance and Infrastructure Protection. However, membership status will not affect the dissemination of credible and specific threat information. Such information will be provided in a timely fashion to potentially affected members and non-members alike.

Maritime target

There is little argument that future terrorist attacks could and probably will be directed at a maritime target. However, the M-ISAC, partnered with the US Government, its allies, international maritime bodies, and the industry it represents, will take a sizeable step forward in identifying threats and vulnerabilities, in disseminating such information to those maritime industry elements at risk and in providing expert guidance in the creation of meaningful countermeasures. The M-ISAC, when coupled with an industry moving in high gear towards comprehensive risk mitigation, is a powerful tool for preventing a maritime equivalent of 11 September 2001.

Contact:
Kenneth P. Bergquist and Kim E. Petersen, The Maritime Information Sharing and Analysis Center

Tel: +1 954 567 2536 E-mails: kbergquist@maritimesecurity.org; kpetersen@maritimesecurity.org
Website: www.maritimesecurity.org