The Role Of Information Exchange On Navigation Safety And Security Enhancement

Ahmed KASSAR and Alsnosy BALLBA

Arab Academy for Science, Technology and Maritime transport
PO Box 1029, Miami, Alexandria, Egypt
kassar@aast.edu – alsnosy222@hotmail.com

ABSTRACT

Information exchange plays crucial role in navigation safety and security implementation, the fast improvement in communication technology, increased accessibility to information channels. Collected information could be used as negative or positive contributors to the safety and security of ships while sailing especially near coastal areas.

International shipping has been identified as vulnerable to global terrorism. Sound security management practices are considered essential if exposure to loss due to terrorism, piracy and other criminal activities is to be reduced. Statistics has shown dramatic increase in incidents involving ship's attacks especially in Far East regions and low social living levels areas around the world. Most of theses attacks have been planned and organized depending mainly on information pre-collected about targets.

Information about ships route, origin, speed, and destination could be used positively by the coast control stations to identify and secure ships and avoid collision or used to analyzing the traffic situation and carry out search and rescue operations. Breaches by unauthorized or illegal gangs to the ship's data could be used negatively to threaten and attack the ship.

Information breaches could threat the ship indirectly by Subversion, Espionage, and Sabotage. Information could be breached whether through person's formal or social relations or through routine information exchange between ships and control stations or through penetration to inboard satellite communication channels.

Shipping companies, port control stations and reporting systems should put clear policies concerning information security, and every one at shore or onboard a ship should be aware of the negative outcomes of information release and the possible ways of breaches and penetrations. Moreover, everyone concerned should know how information release could be used negatively to threaten the company interests or the company fleet itself.

1. Introduction

Easy Information Easy Targeting

Information and data collected or breached plays an important role in navigation safety and security, information collected by the coast control stations could be utilized positively by the authorities using, for instance, AIS (Automatic Identification System) and/or any other regional reporting systems like VTS (Vessel Traffic System) to collect, analyze, and process data in order to enhance navigation safety and security.

Simultaneously, most of accident investigation reports have declared that the majority of ships' attacks have been initiated and built up depending on pre-collected information released during ships` stay at ports, or through

monitoring ship–to shore communications and using intercepted information to select targets. Violent piracy on the high seas has soared and more ships are being hijacked to kidnap the crew for ransom.

The risk of terrorist attacks can perhaps never be eliminated, but sensible steps can be taken to reduce the risk. We cannot continue to hope for the best and ignore the lesson. There was no concern on how ships were targeted? Why at this position? Why at that time? How pirates recognize ships' cargo and identify it? Answering to all of these questions is very easy, of course, because the evil gangs breached the ship's tracking information, and the ship was expected in time.

The International Maritime Bureau (IMB) declared that number of reported ship attacks jumped to 445 in 2003, 20% higher than the previous year and the second highest level since it began collecting statistics in 1991 until 2003.

The number of seafarers killed also climbed to 21, with another 71 crew or passengers listed as missing, while 88 were injured. This compared to 10 killed and 38 injured the previous year. The number of hostages taken also nearly doubled to 359 in 2003.

The figures show an increase in the number of the attacks and violence of the attacks. The IMB said the number of ships hijacked for the theft of the vessel and its cargo had dramatically reduced, but that more vulnerable boats such as tugs and barges were being targeted and crews were being abducted for ransom.

Indonesian waters continue to be the most dangerous with 121 reported attacks in 2003. The Malacca Straits, between Indonesia and Malaysia and one of the world's most strategically important shipping lanes, saw a rise to 28 attacks in 2003. Thirty percent of the world's trade and 80% of Japan's crude oil is transported through the narrow waterway.

Some Western intelligence agencies and maritime security experts have linked al-Qaida, or groups associated with it, to Indonesian piracy. Experts claim al-Qaida showed its seaborne attack capability by bombing the Limburg oil tanker off Yemen in 2002 and US warship USS Cole in 2000. "In 23% of the attacks, tankers were the targets," The following figure showing Monthly comparison of incidents from January to September 2003. (IMB, 2004)

Bangladesh was ranked as having the second highest number of attacks in 2003 with 58 and Nigeria came third with 39. Attacks off Nigeria almost tripled compared to the previous year and the IMB regards it as the most dangerous area in Africa for piracy and armed robbery.

However, some countries saw a reduction in piracy. Somalia had a 50% drop in reported attacks, although the IMB said the eastern

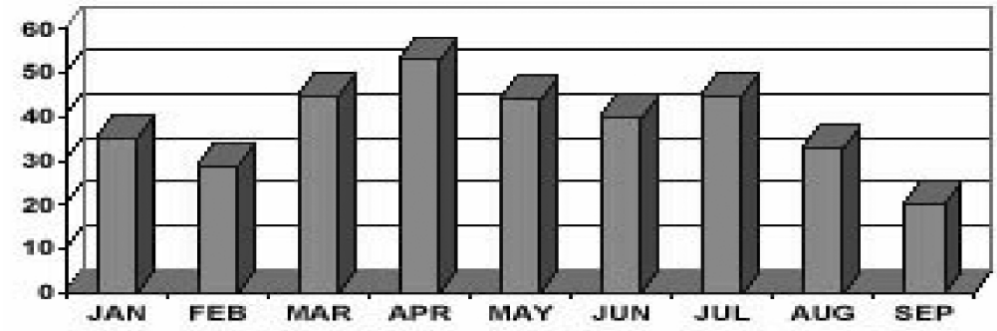

Figure 1 - Monthly comparison of incidents from January to September 2003.

and north-eastern coast of the African country remained a high-risk area for hijackings and kidnapping of crew for ransom. Other countries with fewer attacks in the past year included Cameroon, Ivory Coast, Ecuador, Guyana and Thailand. Malaysian waters saw a fall to only five attacks, with none reported in the last six months of 2003, which the IMB said was due to vigilant patrols by the Malaysian marine police.

Any vessel, not making a scheduled call in a Somali port, which slows down or stops close to the Somali coast, will be boarded by evil gangs. They had extorted substantial sums from owners for the return of the vessel and crew. This indicate the positive side of information exchange, as the ship could be secured if she only reports its arrival, but these reported information should be as well protected against breaches and intrusion during approach.

2. Sensitive information

Sensitive information might include timing (e.g.…departure, arrivals), location of the ship, routes (routes, charts and etc.), crew nationality, ship/port survey, assessments, designs and architecture, security plans and emergency procedures.

3. Sources of Information

3.1 Personnel sources

Information could be communicated by both authorized and un-authorized personnel, either through legal or illegal channels, using means of communications available such as VHF, Internet, and land networks. Personnel working in the coast radio stations, ships` agency and port traffic management stations could release information intentionally or accidentally to their friends and relatives. However, information could be communicated through social relations between those working onboard ships like ships crew or cargo gangs, stevedoring and subcontractors and their relatives and friends who have relations with piracy gangs.

3.2 Cryptographic and computer sources

3.2.1 AIS as information system

IMO carriage requirements for AIS become effective with the latest amendments to SOLAS chapter V on 1 July 2002, and its amendments in December 2002.

AIS System is a dynamic digital broadcast radio carried on vessels. AIS separately broadcasts relevant information about the vessel at regular intervals depending on the vessel speed, maneuvering or operational status, when these broadcasts are received and integrated with an appropriate display, AIS will present real time navigation and vessel traffic information to both mariner in the wheelhouse and at the vessel traffic service center. AIS information could be of security advantages to the authorities in monitoring and control of the traffic approaching or passing through its coastal waters.

AIS has the potential to become the key element for information exchange and will play an important role for the efficient and smooth flow of information among all parties concerned. AIS is also playing an important role to increase the safety of life at sea, protection of marine environment and efficiency of navigation through:

- Detect potential collisions and grounding.
- Allow ships to take proper action.
- Flow without significant additional activities.
- Enhance scope and quality of information exchange

In full accordance with international regulations AIS must provide automatically – shore stations, other ships and aircraft- information including:

- STATIC Data: IMO Number, call sign and name, length and beam, type of ship, location of position fixing antenna on the ship..
- DYNAMIC Data: ship position, time in UTC, course over ground and speed, heading, navigational status ROT (Rate of Turn)..

- VOYAGE RELATED Data**:** Ship's draft, type cargo, destination and ETA, Route plane.
- Safety related data: As needed.
- International functional messages (when needed): Number of crew on board, ship's waypoints, and Route plan report.

3.2.2 Vessel Traffic Services

One of the most important services provided by VTS is Information Service. VTS is enabling essential or necessary information provided to the users, i.e. those on board subject to make navigational decision. Secondly, VTS is navigational assistance through the exchange of information between the ship and VTS stations. VTS also considered as a traffic organization service, used to prevent the development of dangerous maritime traffic situations of an early stage and in fact it regulates the traffic within the VTS area.

The role of VTS in ensuring security is growing in many areas around the world. Handling security related information within the VTS information network, resulted in adding the security organizations such as coastguard organizations to client's list of VTS.

Norcontrol IT, manufacturer and supplier of VTMIS, *"says that under and above water port surveillance and control system, can be integrated with VTMIS and AIS solutions to provide port security officers with vital prior warning at threats."*

Furthermore, the Polling or controlled mode as specified in AIS performance standards, will allow the VTS to interrogate specific data from ships at any time within the AIS coverage.

Adopting of the long range tracking using the AIS, will also improve the efficiency of monitoring the traffic for security purposes by extending the AIS range beyond VHF, using long range communication technology, e.g. INMARSAT, will facilitate the interrogation of ships in the Exclusive Economic Zone and beyond.

Exchanging security related information within VTS networks on regional and international bases will strengthen the control and combating of piracy, hijacking of ships and other crimes or terrorist acts against ships on international basis.

3.2.4 Functions of AIS when integrated with VTS

The type of AIS used in VTS systems is a shore-based device supporting VTS and surveillance services, as specified by ITU recommendation M.1371-1. The AIS base station could perform several functions includes:

- Act as the main link between the mobile AIS stations (onboard ships) and the VTS.
- Act as repeater to rebroadcast the AIS information.
- Managing the radio channels, including the use of alternate channels when AIS1 and AIS2 are busy.
- Interrogate AIS mobile stations, when authorized to do so.

Applying the AIS technology will improve many of the VTS functions, if not all of them, the following will indicate how the information technology may contribute in improving VTS operations, by clarifying the effect of such technology on each VTS function related to the safety, management and control of the maritime traffic.

3.2.4.1 Identification and communication

The use of AIS technology will eliminate the need of voice communication or at least reduce it, which will also facilitate the use of VHF effectively in emergency situations, for non AIS carrying ships and when verbal confirmation is required in certain situations. Moreover it will overcome the weaknesses of the current manual reporting process.

3.2.4.2 Safety of navigation

Information provided by the AIS to VTS operators, as well as the exchange of information between the VTS and traffic and the rapid and automatic update of the information are added value to the AIS application in VTS centres. Such information exchange will improve the situational awareness, and as

a result will have a positive impact of many aspects, which contributes to the safety and quality of navigation.

3.2.4.3 Navigational information

In addition to broadcasting static, dynamic and voyage related information, the safety related messages, which are also broadcasted by the AIS, will provide enormous tools to VTS and ship operators to exchange additional information improving the situational awareness of all parties

3.2.4.4 Aids to navigation

VTS centres use aids to navigation for different purposes such as, marking traffic separations, port approaching, marking or organizing the traffic near a danger to navigation…etc.

A special type of AIS station, introduced by ITU Recommendations M.1371-1, the (AtoN AIS station) when fitted to an Aid to Navigation could provide information includes:

- Identification of the aid to navigation.
- State of health of the navigational aid.
- Tide and weather conditions,

Furthermore, AIS can monitor the performance of the navigational aid, as well as, the collection of AIS data of the transiting shipping traffic for navigational planning purposes. Moreover it could act as an AIS base station repeater.

Additional potential benefit of the AIS is the transmitting of the so called “Pseudo/virtual aids to navigation” for physically non existing objects, which can be used for many purposes such as, marking a prohibited area for navigation or naval exercise area…etc.

3.2.4.5 Broadcasting of DGNSS corrections

Various Global Navigation Satellite System (GNSS) were invented and used by navigators but none of them was as global or accurate as global positioning system (GPS).

The Differential GPS (DGPS) is regular GPS with an additional correction (differential) signal added. This correction signal improves the accuracy of the GPS up to 2 to 3 meters, and made it possible to broadcast it over any communication channel.

Broadcasting DGPS corrections using the AIS by VTS centre, provided with integrity monitoring system, will enable all ships equipped with GPS receivers in the VTS area to navigate with DGPS accuracy, which improves the position fixing accuracy; accordingly it will improve the safety of navigation.

3.2.4.6 Radar target broadcasting

The VTS can attach the information of a non AIS vessel to its radar target and broadcast it as Pseudo AIS target message to other vessels equipped with AIS in the VTS area. This function will allow non radar equipped vessels, which is only equipped with AIS, to view the VTS radar targets, which will increase their situational awareness of all the surrounding traffic, and will enhance the level of safety of navigation in the VTS area.

3.2.4.7 Metrological and hydrological information

The metrological and hydrological information are the most vital information required by the navigators, in order to proceed safely in their voyages. Receiving accurate information at the right time can save the ship, the crew and the environment.

One of the services provided by VTS centres is the information service which includes weather information among other information as specified by IMO Resolution A.857 (20), the AIS can play a crucial role in broadcasting the metrological and hydrological information, such broadcasting will depend on the type and capability of the measuring and processing equipments.

4. The threat

A ship, whether a merchant ship, a fishing vessel or a leisure boat, is exposed to various

types of threats on the high seas, in coastal waters and in port areas. Different factors, among which, the isolation of the ship while sailing or berthed, the relative ease of access to her and the difficulty of setting up her own protection efficiently, combine to make the ship an easy target for attacks. Information collected or breached could be used destructively to threaten ship owner's interests, commercially or attack the ship itself by one or more of the following threats:

4.1 Piracy

Piracy consists of any of the following acts:

(a) Any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
   (i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
   (ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) Any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b).

4.2 Armed robbery against ships

Armed robbery against ships means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, directed against a ship or against persons or property on board such ship, within a State's jurisdiction over such offences.

4.3 Subversion

Subversion means action designed to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens.

4.4 Espionage

Espionage defined as the attempts to acquire information covertly or illegally in order to assist a foreign power and/or attempts to acquire information covertly or illegally in order to assist a political or commercial competitor.

4.5 Sabotage

Sabotage is an act or omission falling short of a military operation, intended to cause physical damage in order to assist a foreign power, further a subversive political aim, or reduce or destroy commercial competition.

4.6 Terrorism

The unlawful use of force, or the threat of force, against individuals or property in order to achieve political, religious or ideological objectives.

4.7 Other threats

- Investigative journalism
- Criminals
- Disaffected or dishonest staff
- Computer Hackers
- Computer Viruses

5. The shortcomings of using AIS in VTS systems

Alternatively, due to its simplicity in use and the wide variety of information provided by AIS systems, all ships in sea area are part of a network. AIS information could be used negatively through illegal sources and channels. At the time being, due to the enormous fast flow of information

"Every Body See Everybody"

However, there is a down side of the AIS to broadcast such critical and comprehensive data of a ship and its cargo to the public, as for the authorities to access information for security checks so can those with evil intent target vessels worth taking over.

Another warring aspect which should be focused on, is the failure of some AIS equipped vessels to update the voyage data, whether intended or not, whilst the navigation details

are updated automatically and the vessels` basic data should remain a constant once it has been input, details of each voyage - primarily cargo and destination - must be loaded in at the commencement of each voyage. Although this is a mandatory requirement a number of cases being identified by VTS stations of vessels arriving in their areas with incorrect information being transmitted.

6. Security breaches in onboard communications

Owing to the increased accessibility to the marine communication and computing systems, the awareness has raised that network and IT security has become much more integral part of the design and specifications of ship's systems. Traditionally, onboard networks and systems have had two means that made them more secure:

Firstly, they are relatively isolated systems. A network device can only be protected from attack when unconnected.

Secondly, many onboard systems were often bespoke. Without insider knowledge of software code and design specifications, it would be nearly impossible to start an attack. The use of COTS (commercial off-the-shelf) hardware and software, and widely adopted standards like IP (Internet Protocol), can make it easier to access a ship's network without authorization, if it is not properly protected and maintained.

Alternatively, many operational functions, such as navigation, were completely independent systems. However, with the use of integrated bridge systems and LANs connect the whole ship's information to the AIS, the on board systems become integrated and connected within the vessel and back to shore.

There are several routes into a ship's system. It is possible- although difficult- for a third-party attack to be launched directly over a communications system such as the satellite link. An increasing number of satellite systems are based on the Internet, so designers need to factor this into onboard system design.

The use of e-mail and Internet on-board for many of the passengers and crew means that the threat of downloading viruses and causing unintentional damage has increased. Many viruses take advantage of the macro scripting languages of normal Microsoft Office software to infect applications, or worse still, the network servers themselves. E-mail viruses could cause a major problem if they were to cause the mail application to send unwanted e-mails over the ship's satellite link.

7. How information could be secured
7.1 Personnel security

Personnel security could be achieved by ensuring that those whose reliability, trustworthiness and circumstances are not in doubt have access to sensitive material. On the other hands, those who may be involved in terrorism, espionage**,** subversion or unauthorized disclosure are excluded. These could be accomplished by background checks, verifiable work history, personal references and security vetting.

Masters should bear in mind the possibility that attackers are monitoring ship-to shore communications and using intercepted information to select their targets. Cautions should, therefore be exercised when transmitting information on cargo or valuables on board by radio in areas where attacks occur. Members of the crew going ashore in ports in affected areas should be advised not to discuss the voyage cargo particulars with persons unconnected with the ship's business.

7.2 Physical security

Physical security could be achieved through access limitation for unauthorized persons, in addition to the following:

- Keep equipment locked when not in use.
- Screened from viewing.
- May require physical protection.

7.3 Cryptographic and computer security

Cryptographic and computer security could be achieved by encoding and decoding messages between the sender and receiver (e.g. secure e-mail), also, encode radio transmissions between vessels. For example, many Inmarsat service providers include sophisticated firewall features. Combined with a secure network infrastructure inboard, these make it very difficult for outsiders to gain entry.

Measures assigned to the ship's IP Gateway, which changes with each communications session, enhance security. Similarly, using tunneling technology and secured encrypted link between ship and shore. Access to the public Internet is governed by central security policies and having just one traffic profile for the tunnel makes the firewall configuration simple and very secure.

AIS information broadcasted should be well protected and kept away of unauthorized personnel or gangs, these could be achieved by limiting the wide variety of information broadcasted and /or coded the information into a certain number each indicate the ship and its cargo, then decoded at the coast radio station into the ship's full data.

However, vessels or a fleet should have an IT and communications security policy. This should stress that all crew need to be aware of the importance of keeping log-in and password details confidential, and that any intentional security breach will be dealt with severely.

REFERENCES

1) IALA. (2001). IALA guidelines on the universal Automatic Identification System (AIS), Saint Germain en laye. IALA, 2001
2) IMO. (2001). MSC/Circ, 623/Rev.2, *Guidance to ship-owners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships*. London, UK
3) IMO. (2002). Assembly Resolution A.922 (22), *the Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery against Ships*. . London, UK
4) International Maritime Bureau (IMB). (2004). *Report on Piracy and other criminal attacks at sea, ICC vulnerability*.
5) Safety at Sea International, (2003). *AIS and its role in security*, July 2003
6) Safety at Sea International, (2003). *Preventing security breaches on board communications*. August 2003.
7) United Nation Convention on Law of the Sea, 1982

BIOGRAPHY

The role of information exchange on navigation safety and security enhancement.

Ahmed kassar

Captain Ahmed commenced his career as marine lecturer at the Arab Academy for Science and Technology and Maritime Transport in 1993. At the moment he is working as first lecturer in the Deanery of Maritime Safety Studies. He has 10 papers and researches published and presented in national and international conferences. He obtained his Master of Science on (Maritime Safety Administration) from the World Maritime University 1997. He has been nominated as regional expert and consultant in the enrollment of experts of Technical Co-operation Committee IMO. He was delegated to the United Arab Emirates coast guards as an expert in marine safety and search and rescue 1998-1999. He obtained a Bachelor of Technology in Maritime Transport Technology in 1994. He has held his Master of foreign going certificate since 1992 and worked as a marine officer for 12 years. He graduated from the AAST&MT in 1981 as second Mate.