National Maritime Foundation

www.maritimeindia.org

Maritime Cyber Attacks are a Reality

Vijay Sakhuja*

7 July 2015

The International Maritime Organisation's (IMO) initiatives to ensure physical safety and security of maritime infrastructure have proven successful and a number of regulatory mechanisms are in place to ensure safe and secure commerce. The IMO is now developing guidelines against cyber-attacks on the maritime infrastructure.

At the 94th session of the Maritime Safety Committee (MSC) in November 2014, a proposal was adopted for 'voluntary guidelines on cyber security practices to protect and supporting the operations of ports, vessels, marine facilities and other elements of the maritime transportation system'. Six months later, at the 95th session of the MSC, it was noted that the Member States, international organizations and shipping industry should 'collaborate on proposals for guidance on maritime cyber security', and submit these by the next session in 2016.

The above initiative by the IMO is noteworthy and clearly suggests that cyber risks to maritime critical infrastructure are real and prevention, and mitigation of these is an important issue for global trade. Ports (vessel traffic management system, cargo data and port operations) and shipping companies (data of cargo, ship disposition, future routing, crew management, etc.) are vulnerable to cyber-attacks. According to one report, the online defences of 16 of the world's top 20 container carriers had serious security gaps. Further, ship-based computers and servers (electronic charts, onboard navigation and propulsion systems, safety and security sensors, other devices and instruments) are potential targets for cyber-attacks.

There are a few documented incidents of cyber-attacks on maritime infrastructure wherein the perpetrators successfully penetrated the networked computing systems. For instance, smugglers hacked into the port cargo handing data and were able to locate the containers with drugs which were pilfered without detection. Interestingly, the smugglers even managed to tamper the cargo manifest and deleted the data of the shipment.

Spoofing, a technique that creates false signals to gain control of the computer system is a major concern for safety and security of shipping. Interestingly, during an experiment to test the penetrability of a ship's command system and the probability of detection of cyber-attack, the students at the University of Texas successfully spoofed the GPS of a yacht.

An industry report titled 'AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea' has concluded that there is a 30 per cent increase in ships reporting false identities for a variety of reasons including cargo and shipping information that can impact on commodity prices. Further, ships have been reported to transmit incorrect position; and in some cases ships switched off the Automatic Identification System (AIS) and the long-range identification and tracking (LRIT), a mandatory equipment fitted onboard merchant ships to transmit their real-time position, 'go dark' to avoid detection for a variety of reasons.

Apparently, the Somali pirates 'hand pick their shipping targets by tracking online the navigation track of the vessel' by breeching into the AIS and the Electronic Chart Display & Information System (ECDIS), a computer-based navigation information system which can be used as an alternative to traditional paper charts. This information was critical for the pirates to track the vessel and launch an attack.

The offshore energy infrastructure such as oil rigs and drilling platforms are equally vulnerable to cyber-attacks. A reported incident of spoofing involved hackers successfully tilting the floating oil rig which resulted in shutting its operations; it took 19 days to make it seaworthy again after computer malware were removed from the computers controlling the rig. According the British government, attacks on energy infrastructure have already cost UK oil and gas companies approximately US $672 million annually and cyber-attacks on energy infrastructure could cost nearly US $1.9 billion to the energy companies by 2018.

Maritime cyber-attacks are of serious concern to both for the maritime industry and the marine enforcement agencies. These can potentially disrupt economic growth and subvert national security. Nearly 90 per cent of global trade is carried over the seas and any disruption of the global supply chains due to cyber-attack can impact 'just in time' cargo supply that can severely affect the production chain.

At another level, fishing vessels switching off the AIS is of immense concern. These vessels are considered 'eyes and ears' and the first line of defence for maritime enforcement agencies, but could be creatively used by terrorist to launch attack. There are also fears of fishing vessels engaging in illegal activities and 'gaming the system and manipulating AIS data'.

While the IMO engages in developing minimum standards for cyber security for global maritime shipping, the national maritime agencies need to engage in cyber security research and obtain a better understanding of the implications of spoofing of the maritime infrastructure. They also require a holistic cyber security policy, which should include specific assessment of maritime cyber risks including other critical assets, which are dependent on maritime commerce. Cyber security awareness and training programmes for shipping companies and port authorities and educating the fishing industry of perils of cyber-attacks would help in prevention and mitigation of the threat.

*Dr Vijay Sakhuja is the Director, National Maritime Foundation, New Delhi. The views expressed are those of the author and do not reflect the official policy or position of the Indian Navy or National Maritime Foundation. He can be reached at director.nmf@gmail.com