Cybersecurity: The Inland Vessels Act, 2021

Author(s):

Mayank Suri

Keywords: Cybersecurity, India, Inland Vessels Act
Read Time: 9

In order to consolidate laws relating to trade and transport by inland waterways, the government of India enacted the Inland Vessels Act, 2021 ("the Act"). When this Act was being tabled in Parliament, the Minister of Shipping said that it was needed for "future technological development, capable of facilitating present and future prospect of trade, transportation and safe navigation."[1] This note verifies whether the Act has sufficiently covered the subject of cyber security by studying its definitions, survey, and classification provisions.

The Act

There are 114 sections in the Act. These sections are divided into 18 chapters. It must be noted that this Act repeals the previous act of the same name which was operating since 1917.[2] It is goal-based. However, the goals are many, ranging from ensuring safety of navigation to ensuring accountability of administration of inland water transportation. In that sense, it is an all-encompassing act that attempts to govern several stakeholders and arguably all their activities relating to navigation on inland waterways.

No provisions for cybersecurity

What is deeply surprising is that even though the Act was formulated and passed in 2021, it lacks a chapter or any direct provision relating to cybersecurity. This lacunae gains prominence in light of international shipping concerns that have been recognised at least since 2017. Notably, the International Maritime Organisation ("IMO") flagged "the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping" in 2017.[3] The IMO expressly asked governments to "expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities."[4]

Definitions and the question of cybersecurity

The Act defines "casualty" as including any vessel which is lost, abandoned, or materially damaged.[5] To the exclusion of cybersecurity threats, "lost" and "abandoned" may be understood in traditional maritime form such as lost due to being wrecked or abandoned by crew. However, with the slight exception of narrowly interpreting damage as physical damage, the term "materially damaged" seems broad enough to cover incidents of loss of

propulsion due to a cyberattack. The other three sub-parts of the definition give a cause-based interpretation i.e. if a vessel causes loss, damage or pollution it will be categorised as a casualty. Again, cyber threats may result in these eventualities.

The next two definitions, although in the context of insurance, provide another reason for the explicit need to address cybersecurity. These are “material fact” and “material particular.”[6] The definitions call upon an insurer to exercise prudence in assessing the extent of their liability. Invariably, hull insurance contracts cover damage to the insured vessel and if it includes a third-party loss clause then damage to the other vessel(s) too. It seems likely that a prudent insurer would assess whether a cyber threat can activate their liability.

The Act also defines a “mechanically propelled inland vessel” as any vessel propelled by mechanical means of propulsion.[7] It does not distinguish between a propulsion disconnected from the cyber connected systems and a “smart” propulsion system. This means that vessels with propulsion connected to navigation, communication, safety, or other cyber connected systems are not excluded from the ambit of the Act and therefore, they can be employed for use in inland waterways while the risk of cyber threats to their propulsion exists. Note that the definition does not state that the propulsion system should be attended to by a crew or that the mechanical means should be started or activated or controlled by a human. This seems contemporaneous with developments relating to crewless vessels.[8]

The definition of “minimum manning requirement” requires that the crew on board should be of the standard and number required for safe manning and navigation of vessels.[9] If autonomous and remote controlled vessels are construed to be “safe” from a navigation perspective, the definition does not require even a single person on board. Although one can appreciate if these terms are interpreted from a precautionary point of view where the presence of an absolute minimum number of crew might be considered necessary. This could be implied from the words “safe manning” in the definition. Even if it seems a stretch to argue that the definition of minimum manning requirement with the element of safe “manning” can be conflated to include crewless cybersecurity measures, this may be possible. The definition of “crew” in the Act makes this clear.[10] It reads:

“crew” means personnel employed for operation or serving on an inland vessel other than master or passengers as a part of performing the functions of manning;[11]

While “manning” is not defined in the Act, the above definition seems to give it a wider berth than personnel. It prescribes that manning is a function. A function of which personnel perform a part. Would a cybersecurity act that is not performed by personnel but by a computer system be interpreted as performing the function of manning, is a question that requires answering.

Finally, there is the definition of “special category vessel” which allows for the special categorisation on a number of factors, varying from “use” to “areas of operations” or “such other criteria or standards.”[12] It interestingly also includes categorisation based on

“source of power for propulsion” and specifically provides for “electrical propulsion.”[13] It is reasonable therefore to assume that the makers of the Act acknowledged and made a provision for modern systems, including systems which would be connected to the cyber world and whose command, control, and navigation can be conducted over the internet.

Thus, the definitions point towards an exposure to cyber risks in several different forms. Loss of propulsion, compromised ship state systems, or manipulation of navigation can lead to a vessel being defined as a casualty. Exposure of insurance to loss due to cyber malpractices inform materiality of the information obligation. Lack of distinction based on connectivity allows potentially even cyber connected ships. By omitting to mention cybersecurity as an element in any definition the chapter has declined prescribing a standard which many may consider necessary in these times.[14]

Provisions relating to survey, classification and the question of cybersecurity

The Act empowers the central government to prescribe the classification, the criteria, and “the standards of design, construction, fitness and crew accommodation.”[15] The Inland Waterways Authority of India (“IWAI”) has been appointed as the representative of the central government.[16] However, the organisation that is de-facto responsible for classification in India is the Indian Register of Shipping (“IRS”).[17]

Neither does the Act nor the rules created under it for survey and classification in 2022 make any explicit reference to cybersecurity.[18] Interestingly, even the rules created for safety of navigation do not include any express reference to cybersecurity procedures or instruments.[19] It is only as an additional service that the IRS offers survey and classification of cybersecurity systems.[20]

In other words, one may understand the cybersecurity aspect as follows. The Act states that a vessel may only operate if it has been duly certified after a survey.[21] However, the criterion for certification have been limited to the type of service and zone of operation of the vessel.[22] Zone of operation is distinguished based on maximum significant wave height.[23] On the other hand, vessels are classified in three categories (A, B, and C) based primarily on size.[24] Cybersecurity has been ignored, by omission, in this chapter and rules thereunder, as well.

Conclusion

The above shows that cyber risks are undermined in the regulatory documents as they currently exist. The effect is that vessels may be classed based on their ability to perform the type of service in a particular geographical area without any consideration being paid to the risks that emanate from poor cybersecurity.

The rules on classification and eventual registration of a vessel neither require nor mandate that cybersecurity must be considered. This omission in a law made in 2021 is worthy of criticism because the organisations capable of assessing those risks had

flagged some major consequences much prior to that.[25] Even on the Indian merchant shipping side there was acknowledgment of the importance of cybersecurity in 2017, much prior to the Act.[26]

Consequently, the lack of cybersecurity may increase the overall risk to the sector by encouraging operations in blatant disregard. This situation is also hurtful to the overall aim of the government to enable and promote inland maritime transport because shipowners may perceive this as a lackadaisical approach to cybersecurity that exposes them to risks.

Although, some sense of security may be gathered from India's global ranking (10th) in cybersecurity by the International Telecommunication Union.[27] The legislature should have taken cognisance of these capabilities within the country, consulted the stakeholders in the domain of cybersecurity, and included it, by express mention, in the Act. This suggestion also stems from a pain point felt by two industries both of which are covered to some extent in the Act, shipping and insurance. Insurers have traditionally been afraid of covering cyber risks in shipping.[28] As drawn out by the definitions, the Act makes it imperative that an insurer judges what is material to their liability but gives no guidance if cybersecurity is material. An inverse inference would result in ignorance of the issue. A situation which can be expensive, both commercially and ecologically.

A note this short can suffer from lack of examination but even at this cursory glance it seems to be writ large that a legislation of this sort, promulgated to govern a sector of immense social and commercial importance, should be progressive and extensive in its coverage of contemporary issues like cybersecurity. It is suggested that the legislature should discuss the relative means and value of amending the Act to include a definition of cybersecurity or publishing rules in respect of cybersecurity as a requirement for classification and safe navigation, immediately.

[1] Lok Sabha, Parliament of India, Motion for consideration of the Inland Vessels Bill, 2021 (Motion adopted and bill passed) 29 July 2021.

[2] S. 114, the Act.

[3] IMO, Maritime Cyber Risk Management in Safety Management Systems, Resolution MSC.428(98) (adopted on 16 June 2017).

[4] *Id*.

[5] S. 3 (e), the Act.

[6] S. 3 (w) and (x), the Act.

[7] S. 3 (y), the Act.

[8] BBC, Crewless container ships appear on the horizon, 24 March 2023, https://www.bbc.com/news/business-64875319.

[9] S. 3 (z), the Act.

[10] S. 3 (k), the Act.

[11] *Id*.

[12] S. 3 (zt), the Act.

[13] Indian Register of Shipping to provide classification services to six Hybrid Electric Catamarans for Inland Waterways Authority of India, https://www.irclass.org/media-and-publications/news/indian-register-of-shipping-to-provide-classification-services-to-six-hybrid-electric-catamarans-for-inland-waterways-authority-of-india (undated).

[14] IMO (n 3).

[15] S. 7, the Act.

[16] S. 6, the Act.

[17] Indian Register of Shipping (IRClass) helps strengthen Inland Vessel legislation, https://www.irclass.org/media-and-publications/news/indian-register-of-shipping-irclass-helps-strengthen-inland-vessel-legislation/ (undated).

[18] The Inland Vessels (Survey and Certification) Rules, 2022.

[19] The Inland Vessels (Safe Navigation, Communication and Signals) Rules, 2022.

[20] Indian Register of Shipping, Guidelines on Maritime Cyber Safety, 2018.

[21] S. 14, the Act.

[22] R. 4(3), The Inland Vessels (Survey and Certification) Rules, 2022.

[23] R. 3, The Inland Vessels (Survey and Certification) Rules, 2022.

[24] R. 6, The Inland Vessels (Survey and Certification) Rules, 2022.

[25] E.g. Indian Register of Shipping, 2.2.2, Guidelines on Maritime Cyber Safety, 2018.

[26] Director General of Shipping, Ministry of Shipping, *Implementation of cybersecurity risk mitigation measures on board Indian Flag Ships*, Circular (Engg) 06 of 2017, 06 November 2017.

[27] ITU Global Cybersecurity Index v4, 2020.

[28] M Suri, ‘Autonomous Ships and The Proximate Cause Conundrum – A Maritime And Insurance Law Tango’, Journal of Maritime Law and Commerce (2020)

Suggested Citation:

Mayank Suri, *Cybersecurity: The Inland Vessels Act, 2021*, Digital Law Asia (Apr. 2, 2024), https://digital.law.nycu.edu.tw/blog-post/zgnvqj/.

PrevPreviousBig Brother Bargain: Can Governments Bypass Your Rights by Paying Up?
NextHe Said, She Said: Who Gaslighted Whom? Decoding DARVO in the Depp v. Heard Trial and the Impact of Social Media on Jury Trial VotingNext