KOCAELI UNIVERSITY
FACULTY OF MARITIME STUDIES

ISSUE 8

OCT. 2025

ELİZYA

SET YOUR ROUTE CORRECTLY

Turkey, which has the most beautiful geographical position and is surrounded by the sea on three sides, is capable of raising the most advanced maritime nation with its industry, trade and sports. We must know how to utilise this capability

M. Atatürk

OUR COSMETİC MEASURES FOR CYBER RİSKS OF SHİPS!

Dr. Aybars ORUÇ
Tallinn University of Technology
Maritime Cyber Security Center

Let me say right at the start: if you are not interested, do not waste your time. This article criticizes the cosmetic measures taken against cyber risks on ships. For years, I have been conducting scientific research on maritime cyber security at universities abroad. Because of this field, I have spoken with many professionals working in the maritime sector. I have examined the cyber security plans in companies' Safety Management Systems (SMS), their risk assessments, the circulars they publish, the posters they put up, and the training they provide. In this article, I will discuss our main mistakes and wrong assumptions.

When people think of cyber security, computers, modems, and routers immediately come to mind. Risks are often seen as malware and weak passwords. IT specialists in companies keep warning everyone: "Be careful when clicking links in e-mails." Of course, that is true and certainly applies to ships as well.

But the cyber risks ships face go far beyond this. Today, ships are equipped with numerous computerized systems to enhance safe navigation and operational efficiency. These systems are spread throughout the ship, from the bridge to the engine room. Yet, while they bring benefits, they also introduce cyber security concerns.

Today, many published scientific studies reveal that various vulnerabilities exist in onboard systems. One of the main reasons for this is the long service life of ships. A shipowner builds a vessel today and operates it for 30 years. So what happens? Systems built with 30-year-old technology are expected to withstand today's cyber attacks. Is that possible? Of course not, it is a big fantasy. But no one is disappointed, because no one is even aware of the cyber risks.

If scientists can find vulnerabilities, do you think attackers will lag behind? Absolutely not. Especially with state-sponsored actors and their vast resources, the maritime sector is increasingly facing cyber attacks. These attacks can particularly impact navigational safety or cause financial damage to shipowners. Such attacks demand urgent attention to the findings and recommendations of researchers. Countries advanced in maritime technologies, such as Norway, take these recommendations seriously, bring them to global attention, and push for rules at the IMO.

The IMO's first rule requires the preparation of a cyber security plan. In other words, IMO tells ship operators: "Your Safety Management System must include a cyber security plan." I open the plan and look inside. I see something called "Radio Navigation Electrical Engineer." I ask, "What is this?" and the manager replies, "I do not know." It turns out that the consulting company they bought the plan from wrote it, and the operators just put it in their system without even reading it.

"They're young boys; they know that stuff"

I keep reading the plan and see they appointed a "Cyber Security Officer" on board. I ask companies, "Why did you appoint this person?" They say, "We heard it was necessary, so we did it." They are acting on hearsay. Then I ask, "Why did you pick the II. Officer as the victim?" They answer, "They are young guys, they know these things." I ask, "Did you provide any extra training for them?" Of course, I already know the answer. A big NO. But on paper, is there a cyber security officer onboard? Yes, proudly there is.

That is not enough, they also appoint someone responsible on the office side. Usually, the victim this time is the IT manager. But IT's main responsibility is not cyber security. It is like this: on ships, deck and engine officers receive some shared training such as maritime law, survival at sea, and firefighting. But their main responsibilities are completely different. The same goes for IT and cyber security specialists. They may share some knowledge, but their responsibilities are worlds apart. Different, but the companies do not realize this yet. If you put that IT manager on the bridge and ask him, "Show me the ECDIS," you would be waiting until morning. I can see this is not going to work with the plan, so with some hope I turn to the risk library. Because this time IMO tells ship operators: "You must assess cyber risks, and I will check when I come." I eagerly search for the cyber risks.

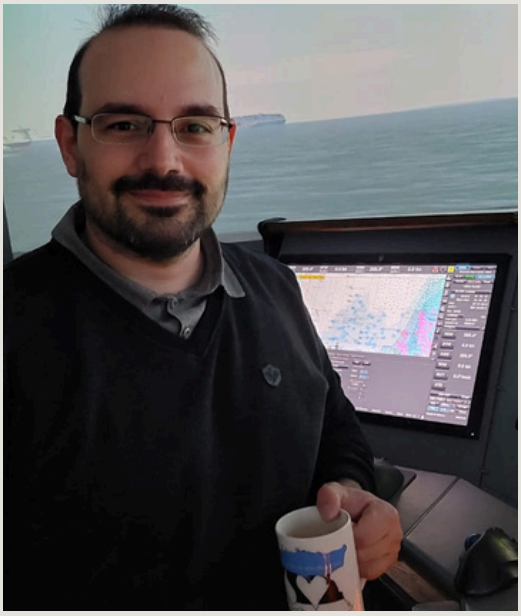
With excitement I find the company's assessment: "There is no internet onboard, therefore, no cyber risk." At last, the magnificent assessment I have been searching for all these years!

Some companies identify risks as "USBs." They slap cheap plastic USB locks on some ports, but only on the ones they feel like, not all. Basically, however many come in the packet. But some companies take it more seriously. They lock up equipment like ECDIS with ordinary keys. They appoint the master as responsible for the keys. If only they did not hang the keys right next to the hat stand, it would be perfect, but we cannot expect them to get everything right.

Naturally, this makes one wonder how they train seafarers. Let me say upfront: today, IMO rules do not mandate cyber security training. But because inspection programs such as SIRE, CDI, RightShip, and TMSA, which are crucial for commercial operations, do require it, such training is delivered onboard in some form. But our training is bizarre. Many maritime authorities argue that cyber security training should be tailored to responsibilities.

For example, teach deck officers about the cyber risks of bridge equipment, and engine officers about the engine control room. Sounds logical, right? But not with us. We give one training, the same for everyone. And the content is simply: “Be careful when clicking links.”

Today, many devices like ECDIS and RADAR run on Windows operating systems. Fine, but are these operating systems ever updated? I go onboard and check the bunker transfer system. Windows XP stares back at me. My friend, your last update was in 2009. Who knows how many vulnerabilities you have. I decide not to mess with those systems and instead check the antivirus software. After all, the company proudly told me they installed antivirus programs. Yes, they did, but they have not updated them. They expect antivirus software that has not been updated in a year to fight modern malware. I hope shipowners’ optimism does not one day come crashing down.



I ask, “Do you receive cyber security consultancy?” They say, “Of course, we get Windows updates for laptops.” They mistake computer maintenance for cyber security service. To prevent forgetting passwords, they stick labels with the passwords right on the devices. And the passwords are “111111.” God forbid they lose it, nobody would ever guess. For updating ECDIS electronic charts (Electronic Navigation Chart (ENC)), they set aside a dedicated memory stick, to be used only for updates to avoid infection. I ask, “Where is it?” They say, “The engineers took it.” I reply, “I know, that is just like them.” After all, I am a former engineer myself, I know how it goes.

I could go on endlessly writing about the measures we pretend to take. But the space kindly offered to me by Dear Eyüp Mazooğlu, who worked on preparing this issue of Elizya, published by the Barbaros Maritime Club of Kocaeli University, comes to an end here. Complaints can be sent to him, praise to me. Until we meet again somewhere else someday.


EVERYTHING
ABOUT THE SEA
/barbarosdenizcilik
/barbaroskulubu
/BarbarosDenizcilikKulübü
Scan to visit our website