Photo: Pexels

Interview with Itai Sela, CEO, Naval Dome

The cyber security seal

by **Przemysław Myszka**

Naval Dome is an Israel-based cyber security specialist providing security detection and protection solutions to the international maritime industry. The multi-award-winning Naval Dome solution is the first maritime multi-layer cyber defence solution for mission critical on-board systems. For more info, please visit https://navaldome.com

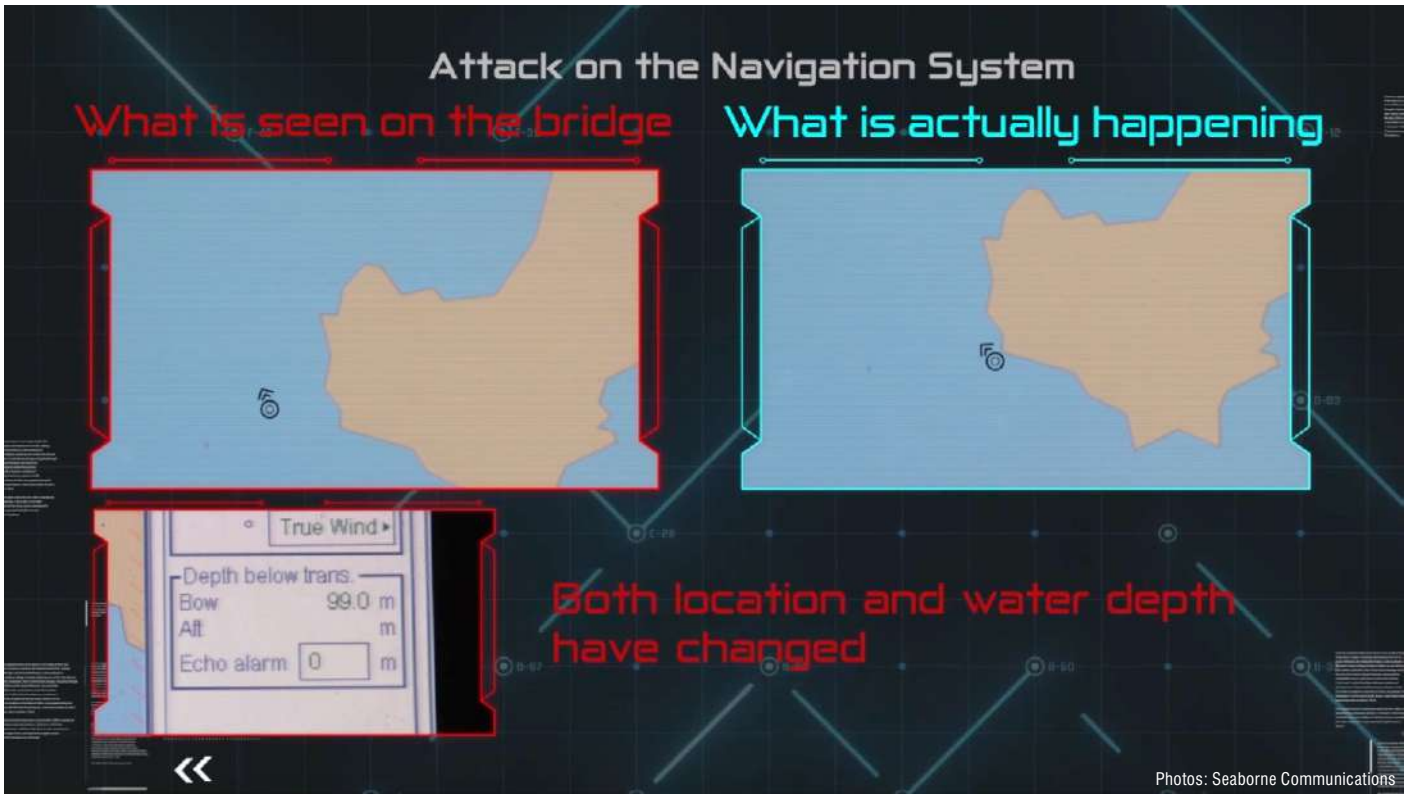
One could almost perceive it as a miracle that the world continues to spin, following all the breaking news on cyber attack, scams, and scandals that cost the global economy billions of dollars each year. Coming increasingly more to the cyber limelight is the transport and logistics industry, until recently somewhat unmindful of the consequences of being too cyber-remiss. We're talking to Itai Sela, the man behind setting up Naval Dome, about the maritime industry's awareness of the threat, what's in the perpetrators' malicious toolbox, and what his company has in store to blunt the potential intrusion.

■ **What's the company's story – why was it established and what are its main goals?**

I'm a former Israeli Navy officer. During my 25 years' service, I recognised a potential security blind spot in the maritime industry, believing if someone can breach a security facility eight floors underground, then it cannot be very difficult for someone to breach a vessel at sea. When I shared such thoughts with the commercial maritime industry, they initially resisted. "The vessel is like an island," they said. "No one can hack a ship!"
Despite that reaction, my team and I were undeterred and looked at developing the optimum maritime security solution, drafting in some of the brightest minds in naval intelligence and cyber security with whom we established Naval Dome. To show the industry the extent of the problem the Naval Dome team first carried out ethical cyber attacks on live navigation, engine, and other machinery control systems, succeeding in attacking different electronic systems from different manufacturers. The breach was carried out in the same way in which a hacker would operate. However, the difference was that the operators and system manufacturers knew of the "attack." Had an actual hacker carried out the same intrusion, they would have had no idea.

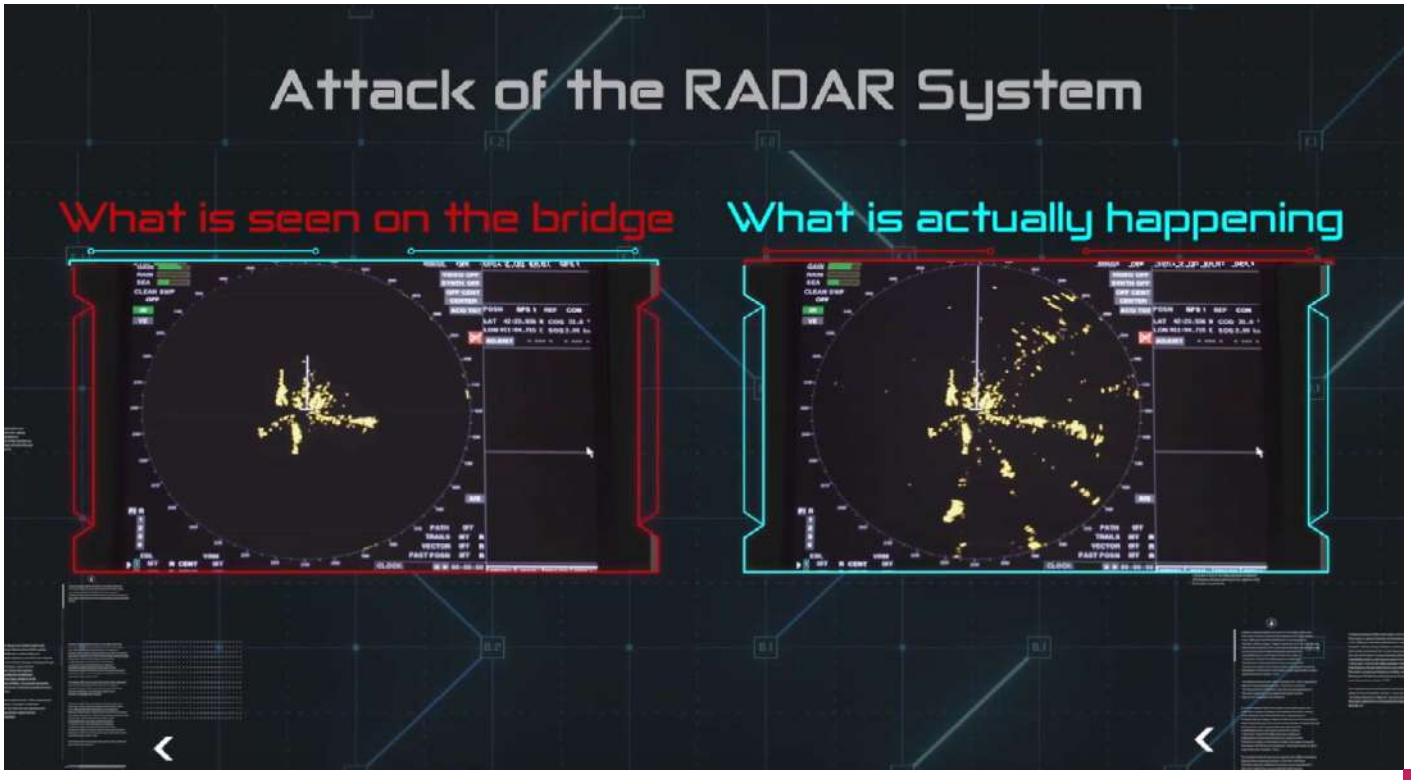
■ **What's in the company's portfolio? Specifically, what is the multi-layer cyber defence solution for mission-critical on-board systems?**

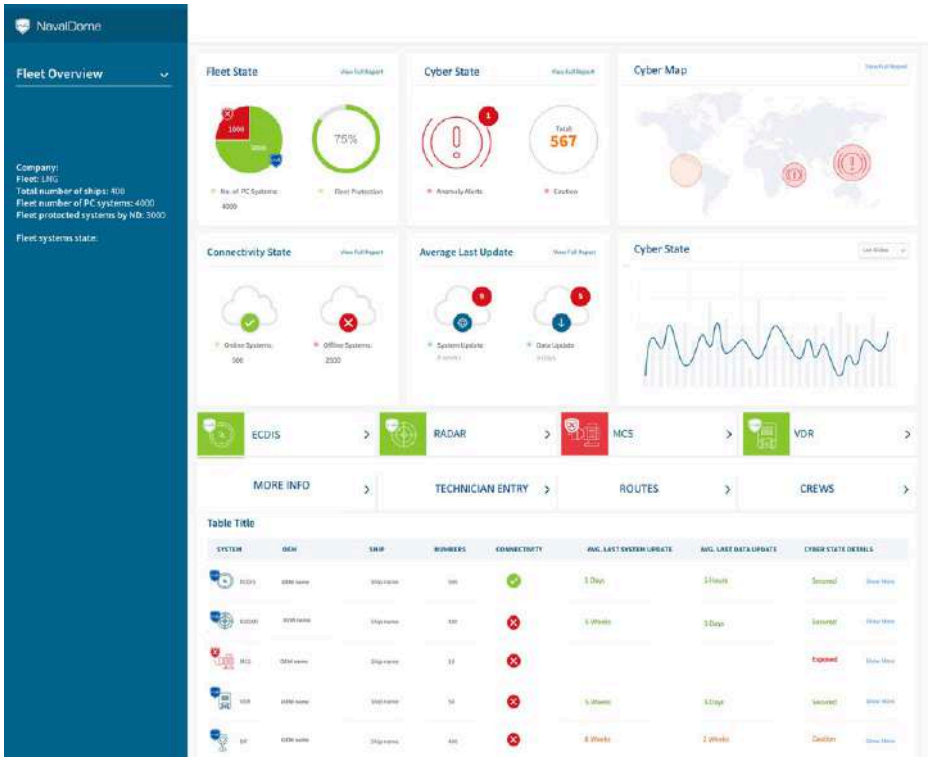
What Naval Dome discovered from these carefully managed attacks was that there wasn't just one blind spot,



there were many. A lot of the systems were unprotected. It was at this point that the team and I began developing the Naval Dome Endpoint solution to deliver the highest level of cyber security for all floating assets. Earlier this year, the company's Secure Endpoint product achieved the highest level of security certification/type approval, Security Level 4 (SL4), from the classification society DNV GL.The Naval Dome solution is a two-step, multi-layered cyber protection system. The first stage, the Secure Endpoint, prevents internal cyber attacks by replacing the on-board systems' hard disk with the Endpoint "hard disk." Once installed, the ship's system functions in the same way, but it's now secured to SL4 grade protection. It can work with different operating systems, including Windows and Linux.

The system also ensures ship operators can assess the security of all systems that have been installed with Endpoint. The Secure Naval Dome App and Dashboard indicated what systems are protected, those that have detected and protected against intrusion, and real-time





security monitoring/alerts for the ship and shore personnel.

The second aspect of the Naval Dome solution is the Secure Naval Dome Cloud. This protects all data delivered to and from the vessel and prevents external cyber attacks. What Naval Dome has done is integrate its own Secure Cloud with the customers' existing Cloud-based infrastructure so only the client's "cloud" is needed.

Today, I can proudly say Naval Dome is the leading supplier of multi-layered maritime cyber defence and analytical solutions. To date, we have secured the PC-based systems onboard a significant number of commercial vessels and super yachts. Naval Dome is working with leading original equipment manufacturers (OEMs) to help protect their systems in a way that it becomes an integral part of suppliers' existing and new software. The OEMs are now integrating the Naval Dome software with the systems to provide their customers with the utmost protection. This is much easier for end users as they only have one point of contact – the OEM – to provide all the service and support. In recognition of our works, we've won several industry awards, including the Marine Propulsion Marine Intelligence Award 2018, Lloyd's List Cyber Security Innovation Award 2018, and the Seatrade Cyber Security Award 2018.

■ What do cyber criminals have in store to target the shipping and port industries?

Typically, cyber criminals will use malware or ransomware-type viruses capable of infecting complete ship networks, and operators will be unaware until the virus has been activated. This is because many of the systems are based on old operating systems and designed and manufactured without considering the cyber risk.

There are two main threats: untargeted and targeted attacks. The former is when someone attacks several companies at once, and the virus spreads until it finds an unsecured network. The latter, in turn, is when specific companies or industry sectors are infected directly.

An attack can be successful when operators make a mistake and inadvertently upload an infected file, e.g., by opening an email or connecting an infected file. This creates connectivity. The second way is when an OEM or technician is attacked, and the infected files are inadvertently spread during system updates or servicing. The second method is more effective in spreading a virus.

■ How the shipping industry reacts to (cyber) security threats?

Unfortunately, the industry has been slow to react, relying mostly on operator training as a precautionary measure. However, reliance on the human factor in the cyber protection cycle is not the answer.

There is also limited control over the vendor's maintenance, updates, and test equipment which could, if they aren't properly protected, inadvertently infect the network. Typically, most networks are not segmented, so if an attack has been detected in one area of the network, it usually means the entire system is infected.

Another aspect that impacts the security of ship systems is that there are no mandatory requirements, only guidelines. There should be binding instructions.

■ What's the company's take on the so-called cyber clause introduced by BIMCO? The clause will require, "[…] the parties to have plans and procedures in place to protect their computer systems and data, and to be able to respond quickly and efficiently to a cyber incident."

The BIMCO cyber clause is very much a move in the right direction, but this does need to be adopted widely. Maritime insurance companies also need to develop consistent and comprehensive maritime cyber insurance policies and remove the CL380, the clause that removes any insurance relating to computer-based problems. Every ship system should be protected to SL4 as well as implement the BIMCO guidelines. Ship operators should also segregate their operational (OT) and information technology (IT) networks. The problem is that these are often connected. There is no real network segmentation. This is very important.

■ What's the company's outlook about how the shipping business will tackle the cyber threat in the near future?

We encourage more and more OEMs to integrate the Naval Dome solution with their systems and equipment prior to delivery to their customers. This way, both the OEM and the end user are confident that their systems are protected at the highest level from the outset. This also means that the end user no longer has to worry about cyber protection as the OEM provides the requisite services and upgrades that are protected by Naval Dome. In the future, all equipment could have the Naval Dome "seal of security," to show that such and such equipment is "Protected by Naval Dome."