Connected Ships and Cybersecurity

Frank J Coles, Transas CEO

Shipping Insight Fleet Optimization Conference

Stamford CT, October 2016

There is little doubt, unless you have had your head under a rock, that you have read about these topics in the maritime market in recent months.

I find the topic fascinating because of my experience in the communications sector and now in the sensors and navigation sector and I see some glaring differences between the two parts of the puzzle – connectivity and the sensors and equipment on board. The difference also has an impact on the discussion relating to remote operation of ships and goes to the heart of the cyber security issue. I am talking about the heavily regulated ship equipment environment when compared to the relatively uncontrolled environment of connectivity. At least in terms of central maritime certification and compliance, which I think is critical to the future, and of compliance in maritime operations cyber security.

The connected ship is like a long chain, with each piece linking to the next and at every point there is the opportunity for a failure or a single point that can create a failure. It can be hardware or software or both and it can be a cyber virus penetration or simply a denial of service, either of which can cause damage.

However, one only has to look in the mirror to see the biggest threat to cyber security. The operator or human represents the largest threat. By nature, humans are gullible and prepared to take risks, we can be lazy or tired and that’s when mistakes will be made. This is something we hear about all too often when we consider the crew on board ship.

If we accept the human as the biggest threat to security, we will probably also then agree that the “cyber missile” that presents itself as being most threatening is the “thumb drive.” No matter where you consider the chain or link weak points putting the thumb drive into an active USB port represents a
significant risk. Nothing really new here, but the essence of cybersecurity is smart information technology system, process and procedures. We have standardisation and regulatory controls for the ships systems and this needs to include connectivity. Aviation is much more advanced than maritime in this respect.

The connected ship is described as many things, your ship, your office. It can also be named the remote managed ship or simply a shared data connection. Before we get to world wide unmanned ship discussions we should recognise the connectivity is not new but we are just getting started in the real use of connectivity in the maritime industry. What is new is the use of the connection in smart shipping. The use we are talking about opens up the discussion about compliance and cyber security to a new level. When we look at the connected ship there are at least 6 places where the link is vulnerable to attack and disruption of service. As with any connection we have the teleport, the satellite, the antenna on board, the hardware in the rack on board as the crucial elements of the connection, plus of course the office and the web. We also have the ships sensors or equipment that may be used to send and collect data.

Everything on the ship is connected to its position, even more so with the discussion about smart operations. It is actually also important to communications; the antenna uses positional data to find the right satellite. I don’t want to dwell on GPS but it also carries some cyber risks.

I do however want to discuss AIS. Automatic Identification System. When I think of AIS in terms of cyber security, I think of Attack, Infiltrate and Spoof. Our industry has seemed to have a complete blind spot to AIS. This is a system that has regulatory controls for its design, the IMO and IEC require compliance for its design and manufacture. However, this is only good insofar as it was designed to be used. It is easy to hack, it is open to spoofing, open to hijacking and open to service disruption. This anti collision device and identification device is a window into world maritime trade. There is a plethora of services being offered on the back of AIS data and while this seems great, the inherent cyber weakness provides the potential for large economic and environmental damage to arise. I don’t think it is wise to speculate too much on this. Suffice it to say, it is quite possible to move a ship, hide a ship, add buoys or objects and create false tracks of ships. What if you spoofed a ship showing it staying on track while all the while it had been hijacked, or driven onto the rocks?
Having mentioned AIS I would like to refer to the ships navigation system and look at the ECDIS. The architecture of a connected ECDIS requires a VPN, two firewalls and user authentications to ensure the security of the ECDIS and the multi functional displays on the bridge. The cyber security is well established. It is controlled through regulation, compliance and strict certification on a global industrial basis by the IMO and IEC. All manufacturers have to comply with the same standards. The costs of compliance for making equipment changes or connection changes are over $100,000 per incident. Just changing the router or connection box in the connected ECDIS requires a new certification process. The connectivity of the smart ship is not subject to this type of industry compliance and control.

If we look at the connection from ship to shore or the connectivity part of the smart ship. There is no standard for the teleport, the satellite, the antenna and the communications rack on board. There are international maritime standards for GMDSS or AIS, but for the big data connection nothing exists. This means the cyber security risk is left to each satellite operator, each service provider and each hardware provider. If we are to have an accepted level of cyber security for the connected ship and the smart ship and even move to a remotely operated ship this will have to change.

An ECDIS can operate without a positional input, it simply uses DR. The antenna on board the ship cannot do this as it is dependant on the GPS input. So the move towards the remote or unmanned and smart ships will require the fidelity of the connection, the robustness of the positional data and compliant equipment to IMO/IEC standards yet to be put in place. We are not there yet and not even close. GMDSS equipment and service has to comply with an IMO/IEC regulatory compliance, but this does not exist for the various VSAT services or Inmarsat FBB and FX or Iridium equipment, teleports or associated hubs and routers. It seems a little odd to have the equipment and services for navigation strictly comply with a set of standards but not the connectivity link in the chain.

One other tangential point on the connected ship and cybersecurity. We are seeing growing demand and use of the Fleet Operations Centre ashore, operating alongside the Vessel Monitoring Services of the various government bodies. For this style of operations going forwards the security of the connectivity is going to be very important. We are also going to need contingency plans in the event that the link is broken. This is where the human
will become important, both on board and in the monitoring centres, as they will be able to communicate with each other and maintain a safe environment.

It is time for the IMO to apply the same standards of compliance used for GMDSS, ECDIS and other bridge equipment to the standard communications networks and equipment. If these networks and the associated equipment is going to be used for operational, remote management and technical decision making it must be cyber secure and compliant with a global set of international maritime standards. Until then we will have a cyber risk associated with a non standard approach to connectivity.

-----------------------------