

THE FRENCH NAVY AND MARITIME CYBER DEFENCE

Given the increasing importance of cyberspace in maritime operations and activities, enhanced information security systems have now become a necessity for the entire maritime sector. Recognizing this reality, the Navy considers cyber defense as a full control field.

The "Cyber Defence Pact", presented by Jean-Yves le Drian in February 2014, reflects the new global momentum for cyber defense in the spirit of the 2013 white paper on Defence and National Security. The French Navy Cyber Defence Support Centre (CSC) was created in this context.

CYBER DEFENSE SUPPORT CENTRE

With units at the forefront of technology, using a variety of information systems, the Navy has fully grasped the cyber issues when creating this specific unit with inter-organic vocation. Under the authority of Vice Admiral Anne Cullerre - representing the Chief of Staff of the Navy for the implementation of joint cyber defence guidelines - CSC's mission is to provide Navy air forces with all the training in this new conflict area.

Training exercises are conducted on board of the units and on dedicated platforms. In addition, CSC has capacity for running exercises (CATAMARAN - GABIAN - DEFNET). Operationally, it is also able to provide rapid response groups capable of being projected on a ship to strengthen it. The objective is to ensure the ability of naval units to detect cyber threats, identify technical and operational consequences, curb, then return to a nominal situation. The training platforms will be split between two sites, in Toulon and Brest.

MARITIME SECTOR DEPENDS ON CYBERSPACE

Issues related to cyber defense nonetheless go beyond just the military: the use of cyber technologies actually relates to the maritime industry as a whole. Several major trends explain this link, including the growing dependence of the marine environment on on-board electronics, the computerization of systems and the growing networking of ships, ship owners and ports.

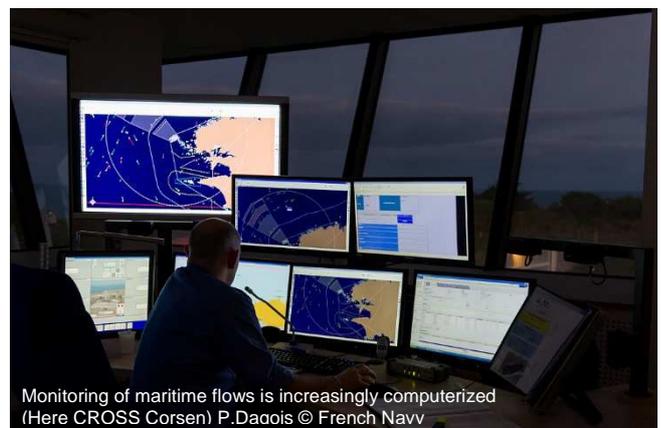
This integration of computer systems in managing and empowering operations related to maritime activities is called "marétique" in French. Its use increases the productivity and fluidity of the maritime sector which derives a considerable profit from it. However, the massive use of new information and communications technology (NICT) sometimes happens at the expense of the security of information systems

A PARTICULARLY VULNERABLE GROUND

While 80% of the "marétique" is based on wireless technology, maritime information systems have long been considered unbreakable. However, technological progress has now made the threat of intrusion and cyber attack a reality, through electronic hacking of GPS or maritime activity management software. In this sense, the hacking of the inventory management software of port of Antwerp, which took place between 2011 and 2013 is significant: it allowed the diversion by drug traffickers of several containers. The attack and manipulation of computer data relating to ships and their cargo is another challenge, as well as falsification of identity – as demonstrated by the example of the *Ramtin* tanker, in October 2013, which was able to thwart the embargo on Iranian oil. In the future, computer hijacking of vessels could be achieved for terrorist purposes.

Computer crime and the use of cyberspace infrastructure as a weapon are the major threats facing the maritime world. But the cyberspace network is much larger than it appears: submarine fibre optic cables - for the transmission of communications and the intercontinental transport of Internet data - through cloud computing and associated data centers - for storing information – reveal increasing marine sector vulnerabilities and require a growing effort to secure.

The Navy will thus have an increasing role to play in the protection effort of the maritime sector. The CSC will contribute to spreading its influence among the various community stakeholders.



Monitoring of maritime flows is increasingly computerized
(Here CROSS Corsen) P.Daois © French Navv