Mr Wolfgang ROEHRIG,
Project Officer Cyber Defence, European Defence Agency (EDA)

Short Curriculum Vitae (C.V.)

Wolfgang Röhrig is the Programme Manager Cyber Defence of the European Defence Agency (EDA). He was born 1966 in Germany and entered the German Navy in 1985. After completing his studies at the University of the Federal Armed Forces in Hamburg with the degree of MBA in 1990 he served in several officer's positions in the German Navy and the German Joint Services including several operational deployments and service in NATO. He bears the military rank of a German Navy Commander. March 2012 he joint EDA as Project Officer and became programme manager cyber defence beginning of 2014. In his current position he is inter alia responsible for the identification of capability gaps with respect to cyber defence in EU-led military operations, and the development and implementation of solutions for closing these gaps through cooperative projects with EU member states.

"Sea Lines of Communication – Does cyberspace create new (virtual) Choke Points in the maritime environment?"

On top of EU Cyber Security Strategy from 2013 the EU Maritime Security Strategy is one of the first international strategies that addresses Cyber as a threat to maritime security. Areas of concern should be: ports, ships and choke point monitoring and control.

Ports; In modern ports the loading, unloading and distribution is done with autonomous or semi-autonomous systems, which are connected around the world through cyberspace with other ports, ship owners, trading companies to ensure a seamless and swift data exchange and with that swift and seamless trade.

Ships; Vessels at sea are connected via a plethora of communication links. Navigation is today widely reliant on electronic solutions. Marine engineering systems are remotely maintained and also radar systems are today software based. All these solutions are moving to IP based data and information exchange and trade at sea will move towards remotely piloted vessels or even fully autonomous and automated ships.

Organisations in place to manage and control the dense traffic; They also use a diversity of monitoring and communication systems to manage the dense traffic and modern IP based solutions are growing in order to allow centralized, remote or even autonomous controlling.

In consequence all three elements are part of global cyberspace. Even more concerning is that international shipping is not only reliant on the full availability of the digital spectrum but this in combination with full availability of the electromagnetic spectrum. Thus, one can target shipping either through manipulation in the electromagnetic spectrum as well as the digital one or a combination of both.

In Cyberspace there is a variety of actors with different objectives and the same traditional motivations for which shipping was target of attacks in the past centuries. Although so far no serious attacks happened to global shipping, incidents in other domains have shown that also the maritime system bears similar vulnerabilities. It is of critical importance to move to a dynamic risk based approach also in the maritime domain to protect against cyber threats applying a balanced set of:

1. State-of-the-art Cyber Security Technology,
2. Cyber aware and savvy personnel, and
3. Right processes that bring technology and people together in an effective and efficient manner.