G7 HIGH LEVEL MEETING ON MARITIME SECURITY

Rome, 20 November 2017

THE NEW FRONTIERS OF TECHNOLOGY AT SEA: HOW SECURITY FOLLOWS

A science-to-policy message

Today, security at sea needs to respond to technological challenges that mainly target areas of marine surveillance, recognition of small objects at sea and their classification between potential threats or legitimate objects, secure data sharing, and messaging real-time alarm. Commonly used technologies often have no intrinsic safety features; an example is wireless communications that are, by their nature, subject to cyber-attacks. Safety and efficiency at sea are driven by the use of new frontier technologies that must guarantee intrinsic security in their use. Future developments in the following areas will exert a significant influence on the overall maritime security.

1. ***Secure communications and data (cyber security)***. Important systems for the security of a vessel are vulnerable: positioning systems (GPS, electronic chart display, information systems, dynamic positioning systems), communication systems (satellite, VOIP equipment, WNLAn, public addresses and general alarm systems), bridge systems (all those systems that interface with the electronic/navigation/propulsion/maneuvering systems), access control systems (locks and login credential, passwords, etc.), and cargo management systems are prone to cyber-attacks. A step towards increased security could be to replace Wi-Fi with Li-Fi systems, by using the VLC (Visible Light Communication) protocol.
2. ***Autonomous vessel management***. Developments towards unmanned and autonomous vessels are a solution to meet the three major challenges of the maritime transportation industry: a) to keep operational expenses as low as possible, b) to reduce environmental impact and emission of greenhouse gases, and c) to remove trivial operational tasks and release crew for more complex operations. Unmanned/autonomous vessels act independently within a certain degree of freedom, but they need to be constantly monitored by a shore-based or a mother-ship-based control station. The issue of secure communication protocols for data transmission is vital. Unmanned vessel also need to be able to autonomously solve possible maintenance and/or structural problems.
3. ***Secure storage of data***. The massive amount of data collected from sensor networks, GPS, augmented reality, weather data for area & route, etc., besides being collected and transferred safely, must be stored in safe places for big data processing and analysis.
4. ***Evolved security systems.*** Crisis management can be made more efficient by using: a) computer vision techniques operating in indoor and outdoor environments, b) multisensory biometric recognition techniques for selective access to specific

vessel's environments (fingerprint, voice imprint, face recognition, etc.), c) methodologies for detecting locating and tracking people in a closed environment. New safety and security systems also include sea life assistance and rescue systems based on the development and integration of coordinated drones or/and independent marine robots integrated with a sea-based recognition and tracking subsystem.

5. ***Advanced space monitoring systems.*** Despite being a key resource for maritime surveillance, in particular in high seas where they are the primary information resource, satellite systems have so far limitations in ensuring continuous information on events undergoing rapid changes in short timeframes. Current systems compensate by resorting to complex architectures of constellations of satellites, as is the COSMO-SkyMed system capable of ensuring very short revisit times. A satellite radar system on a geostationary platform would bring a paradigmatic shift in maritime monitoring, allowing a new class of monitoring applications.

Other technologies, while directly aimed at improving safety of operations, can also have indirect security implications by offering possible breaches or vantage points to potential attackers:

1. the use ***of augmented reality techniques*** aimed at improving control and management operations and helping watch officers with visual clues on potentially dangerous situations.
2. ***simulation-based design of ships*** through new mathematical simulation techniques that allow performance-based engineering approaches to demonstrate that an alternative design solution guarantees the required level of safety.
3. the use of ***metamaterials***, which are an arrangement of artificial structural elements, designed to achieve advantageous and unusual electromagnetic properties. As an example, the negative refractive index of the metamaterial makes it suitable to be used for the concealment of aircraft or ships to radar and optical radiation.
4. ***additive manufacturing***, or 3D printing, for ship/maritime repair during the navigation.

The **keywords** in the horizon of the new technologies for security at sea are:

- ***Integration*** of heterogeneous technologies;
- ***Interoperability*** in exchanging data using specified data formats and communication protocols;
- ***Secure*** ship-to-ship, ship-to-shore and shore-to-shore ***communications***.