infodas
connect more. be secure.

Of warships and cybersecurity: the challenges of modernization in times of digitalization

Of warships and cybersecurity: the challenges of modernization in times of digitalization

Dr. Fulvio Arreghini

Navies are constantly modernising their fleet through digitalization programmes. To take advantage of new communication technologies and their numerous benefits such as real-time decision making and information sharing, former air gapped systems are being connected with the IT world. Consequently, sensitive networks are being integrated with less secure ones.

Modern warships are designed to take multiple roles and to operate in a multi domain and highly digitized space, in a continuum of competition, where data are essential for Decision Dominance.

The battlespace of today's of multidomain operation is interconnected and while this increases the efficiency and effectiveness in military manouvers, it also opens windows of opportunities for new threats coming from the cyberspace.

Countering these new threats, while allowing the digital transformation of the battlespace, requires rethinking the way data are moved and transferred through security domains. Cross Domain Solutions are today the answer to this challenge.

Digitalization of warships: Not only Combat System

In the early days of the so called 'combat system' (CS), the metaphor of the Archer was often used to explain its governing concept: the eye of the archer, seeking for the target and then aiming at it was the sensor suite, the brain of the archer symbolized the tactical computer and finally the arrow was the effector, shooting at the target. This clearly revealed how the 'combat system concept' was intended at the sensing, tracking, engaging and neutralization of one or more targets. These functions were often referred as C2 (Command and Control).

The concept of CS has evolved in the Combat Management System (CMS), designed not only for engaging targets but also to provide an number of functions supporting the Commanders in planning and executing the ship mission in the C5ISTAR domain (Command, Control, Communication, Computer, Cyber, Intelligence, Surveillance, Target Acquisition and Reconnaissance), often inter-operating with allied assets in different physical and information domains, as required by the Multi Domain Operation doctrines. The recent interoperability exercises between fighters of three different nations are a clear sign of how the military operation are going to look like in the next decades.

Digitalization in warships made its move above and below the flight deck, OT (Operational Technology), governing core functions for the survival of the Warship such as power distribution system, cooling, sensor and communication suites, remote maintenance systems are as critical as the CMS for the success of the mission. They have been also evolving in more and more digitized systems and are today fully integrated with the CMS.

From NTDS to integrated architectures

The first steps in the digitalization of warships happened in the 60s with CS based on NTDS and centralized architectures. While these may seem obsolete, they are still widely used.

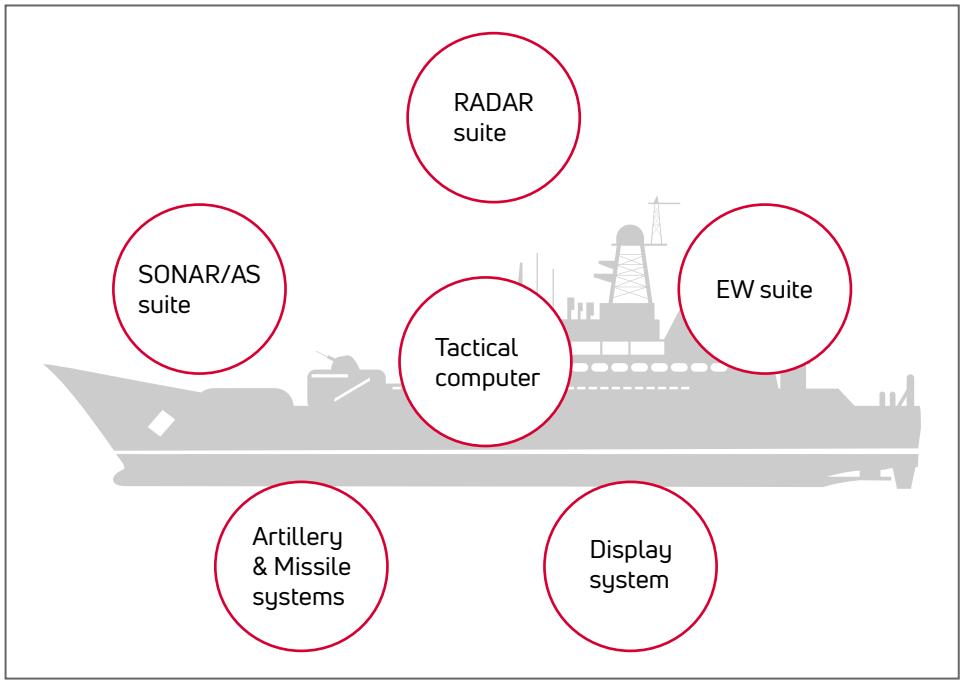

Figure 1: combat system centralized architecture
Source: Own figure

In 1994 came the US DoD decision to adopt Commercial off the Shelf (COTS) technologies, widely known as the Perry memo. The transition to COTS triggered the adoption of commercial standard protocols also in the Combat Systems: the data started to flow between combat system nodes in IP, ethernet, ATM, FDDI, which are all protocols which can be largely found also in the industrial world. The combat system design and especially its integration became then easier and bottlenecks due to format converter strongly reduced. The availability of multiple data sources in a consistent format over a unique bus enabled the data fusion. This shift was the begin of the Federated Architecture adopted in the AEGIS Combat system, and in many other CMS in service today.

The governing paradigm of modern CMS is the Integrated architecture. The CMS , the sensor and communication suites, the Platform Automation (Operational Technology), the logistic systems are integrated in a common framework producing and moving significant amount of data to support timely and informed decisions of the Commanders. The modern Naval Cockpit of the Italian PPA vessel is probably the best example today of this paradigm.

Figure 2: the PPA cockpit
Source: Marina Militare Italiana

Multi Domain Operations

In the 90's the importance and benefits of networks and communication technologies was declined with the concept "network centric warfare", interpreted by NATO in the Network Enabled Capability (NNEC).

Today's multidomain operations recognized that it is not the Network to be the center of operations, but data. Decision Dominance as the ability for a commander to sense, understand, decide, act and assess faster and more effectively than any adversary[1] requires data having the so called 5 Vs (Volume, Variety, Velocity, Veracity, Value)[2] to be constantly moved to reach timely the point where the can provide real value.

Moving data requires connecting security domains. The lingering borders between the physical and the cyber battlespace, are redefining concepts like space, time and security. Assets geographically located hundreds of kilometres far away from the fire of the battlefield are just milliseconds away from it in the cyberspace and subject to ubiquitous cyberthreats.

Figure 3: Ship communications

Source: Naval Post, https://navalpost.com/what-is-network-centric-warfare/

1 Freedberg, Jr., Sydney. "Army's New Aim Is Decision Dominance." Breaking Defense, March 2021.

2 Anuradha, J. „A brief introduction on Big Data 5Vs characteristics and Hadoop technology." Procedia computer science 48 (2015): 319-324.

Ships are not new to cyberattacks targeting communication and position technologies, such as the GPS and the Position, Navigation and Timing Systems (PNT): Spoofing or jamming PNT have been observed , for example, In January 2016, two US patrol boats sailed because of manipulation of their PNT into Iranian waters and in 2018 when hackers breached into some US Navy contractors to steal information. Universities working with the US Navy and the number of cyber attacks is expected to increase.

Cross Domain Solutions supporting Decision Dominance.

So far, the use of air gaps has been the preferred solution to safeguard different security domains. The traditional air gap has for decades been implemented with the use of removable memories manually transferred by operators between security domains or systems. This technique, which is still perceived as secure, has nevertheless more than a problem:

- It is not scalable, as the amount of data to be transferred grows exponentially in volume and the number or required transfer increase, requiring a significant pool of resources.
- It is prone to human error, as the number of data to be transferred and the frequency of transfer increases.
- It does not provide real accountability (Auditability): the data are checked out from the source system when copied on the removable memory and then checked in on the destination system when imported. What happens in the meantime and when the data are at rest in these storage devices cannot be logged or audited and the trust anchor is the loyalty and reliability of personnel. The loss of a data storage device can hardly be investigated if a security accident happens.

What could be called the 'second generation air gapping' is the use of VLANs to segregate data between security domains. Information are segregated by manually moving network cables on the switches (or reconfiguring the VLANs on the switches). This solution, which has the flavour of the telephones systems of the 50s, still has several evident weak points in scalability and security.

Cross Domain Solutions (CDS) represent today the best answer to the numerous cybersecurity challenges met by the navies and industries throughout the designing of new warships, automated or not. CDSs are appliances enabling reliable data exchange between different security domains.

Diodes allowing unidirectional transfer only are to a certain extent known and employed in some parts of modern CMSs. Sometimes, but nowadays, Security Gateways allowing bidirectional exchanges are also available and constitute the state of the art of the technology for securing the border between security domains. Security gateways are able to provide, in arrangement with a small form factor and SWAP footprint, a high level of security in terms of Confidentiality, Integrity, Availability of data and Accountability of operations.

Security gateways can inspect the data passing through them and enforce the organization security policies, coded in the gateway, as a set of security rules. Both Security Gateways and Data Diodes are available in versions approved for NATO/EU SECRET information.