Note n°52/20

July 6, 2020

Nicolas Mazzucchi
Research fellow
Fondation pour la recherche stratégique

Cyber, a particular field of naval thought

This note was originally published in Etudes marines, Issue 17 (January 2020) – *https://cesm.marine.defense.gouv.fr/images/etude/EM17_-EN__NUM.pdf*

In 2019, for the first time, the annual DefCon conference – now in its 27th edition – included an area called "Hack the Sea", dedicated to cybersecurity issues in the maritime sector. Such events highlight the growing importance of the cyber issue for sea-related sectors (military, energy, fishery, transportation, etc.) where the ever-increasing integration of communicating systems into naval platforms has given birth to "cyber-at-sea".

This vision extends to both the civilian and the military maritime domains, as ships must constantly transmit and receive data, over both long and short distances. While the problem of naval communications is far from new, it has undergone a major change in recent years with the growing importance of networked combat capabilities, at the level of both naval groups and each vessel individually. These communication challenges are now included in the cyberspace domain, coming with both new capabilities and new threats.

The aim here is to consider cyberspace in a broad sense, as a particular domain of combat within the maritime space, and also as a technological sector that includes autonomous robotics, artificial intelligence and connected devices. All these technologies rely on data exchanges – permanent or not – among several platforms. In this sense, many current or prospective technological developments fall within the definition of cyber within the armed forces. The announcement of the commissioning of 1,200 drones in 2030 by the French Navy Chief of Naval

Operations (CNO), Admiral Prazuck, for example, requires considering the related cybersecurity issues as one of the core elements of their integration within Navy units. And even beyond the integration of technologies within ships, the question of integrating the cyber domain into naval strategy is all the more relevant because, while some elements seem similar, others are opening up new challenges.

Cyber-at-Sea: the challenges of technological integration

Integrating a cyber layer into sea objects moving above and under water is a much greater technological and economic challenge than deploying telecommunication networks ashore. The use of cyber technologies onshore has grown exponentially over the past few years, thanks to major advances in logistics linked to high-speed networks and the growing popularity of appropriate terminals. In parts of the world, such as Africa, mobile broadband has enabled the widespread use of cyberspace. In the space of ten years, from 2007 to 2017, the proportion of the world's population using the Internet increased from 20 % to nearly 50 %, in line with mobile broadband subscriptions (from 4 % to 62 % over the same period), according to the UN[1]. Networks (3G, 4G and soon 5G), terminals, telephones and tablets have enabled this global expansion – but their promise of optimal and continuous coverage is based on installing fixed infrastructure at relatively short intervals. Thus, broadband telephone base stations have emission radii ranging from a few hundred meters to around 30 kilometers, which imposes a relatively tight mesh of the territories. Other wireless remote connection protocols are also limited in reach: WiFi (IEEE 802.11 standard) has a range of a few hundred meters, WiMAX (IEEE 802.16) – about 10 kilometers, ZigBee (IEEE 802.15) – about 10 meters.

In this context, the maritime domain – where the kinds of fixed communication relays available on land are not possible – is much more demanding when it comes to connecting to cyberspace. Maritime platforms rely mainly on satellite technologies to provide data links for voice and image communication, navigation, etc. In France, cyber links are operated through *Inmarsat* systems for civilians, and *Telcomarsat* or *Syracuse* for the military. Satellite links in the cyber domain are extremely uncommon, about 10 % of global communications, mainly because of their cost. Maritime cyber is thus much more expensive than terrestrial cyber, particularly in the communication aspect, thus forcing embedded information systems to process as much information as possible onboard ships[2].

This situation does not prevent the very fast development of “cyber floating objects”, however. Cyber offers the promise of optimizing the functioning of systems through the use of technologies related to data collection and processing. In this context, the maritime world appears to be particularly relevant for the deployment of cyber systems designed to optimize the operation of ships. Like any “industrial” system, a ship must be able to handle a number of tasks related to its missions in the most automated possible way. In the military context, these range from propulsion to combat missions under the sea and above the surface. Cyber can play an even more important role in this context because it is both suitable for the integration of multiple different subsystems – a ship being first and foremost a systems-hosting platform – and

[1] World Bank and International Telecommunication Union data.
[2] It is partly this logic that explains why the maritime domain saw the commissioning of the first automated weapon systems, such as the Aegis system in the United States (see P. Scharre, *Army of None*, New York, Norton, 2018).

because it allows human gains, and therefore space savings. This is a fundamental paradigm shift in the naval field. Where it hitherto was based on the scarcity of communication, it now is moving toward abundant communication, at least locally or at short range.

Thanks to this advanced automation, ships – military or not – have gained ever more important functionalities. The current *FREMM* frigates have a crew of just over 100 sailors with an operational range of 6,000 nautical miles and an extremely wide range of missions. Their ancestors, the *Tourville* class frigates, had a crew of nearly 300 and a range of 4,500 nautical miles. The more than 30 years that separate them is the time it took to enter the digital age. The ships that have entered service recently are floating industrial control systems, often supported by multiple protocols, making them complex multi-sensor information systems – a kind of connected factory at sea.

In the field of maritime economics as well, cyber technologies offer particular advantages that need to be taken into account, particularly in terms of predictability. One of the major advantages of the digitization of "industrial" systems is the ability to anticipate, thanks to massive datasets that enable better anticipation of flows and improved global logistics, which is essentially maritime. In addition, the autonomous ship, for which research is already well under way within the International Maritime Organisation[3], offers fascinating promises in terms of the logistics for the future, with significant savings in human capital and fuel. However, the emergence of large autonomous systems on the seas raises many questions in terms of technological maturity and safety and legal liability, particularly with systems that would use artificial intelligence.

Beyond the ship itself, with the evolution of missions and needs, the cyber-naval environment is being increasingly integrated with secondary or remote platforms, such as aerial or underwater drones. With these new devices, surface ships (and submarines in the near future) are no longer just floating information systems, but also the core of local mini-networks. The growing number of sensors deployed in unmanned platforms, designed to give the ship a greater visibility of its environment, thus transform the future military ship – and some civilian ones – into a gateway for connected objects. In the same way, as new and future generations of aircraft (F-35, SCAF, etc.) are designed as the center of a system in the air domain around which autonomous sensors/ effectors evolve, the ships of the future will be above all gateways for processing the Internet of Things, probably also acting as data centers[4].

This vision is reflected in the French CNO's speech where he referred to the rapid development of on-board UAVs that can be used in many missions in the maritime field (ISR, combat, electronic warfare, mine warfare, etc.). Thanks to drones, in swarms or not, combat ships could thus become extended multi-mission platforms, capable of covering a much larger three-dimensional territory (air, surface, submarine). This integration of new sensor-effectors would have a dual effect, providing a partial answer to the dilemma of territorial control and the puzzle of naval strategy, and at the same time creating new risks and strategic challenges related to digitization.

[3] http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

[4] With regard to the issue of cyber connectivity, the relevance of the cloud arises much more in the naval domain than in other domains. Hence a processing as close as possible to the sensor according to the so-called *fog-computing* or *edge-computing* model.

Naval and cyber strategies: common issues

A matter of territory

The two spheres – the sea and the cyberspace – have a number of similarities. Among these is the question of the permanence of control over a territory that is essentially considered as fluid. Both in cyberspace and at sea, it is impossible to have continuous control over all territories, notably due to the impossibility to ensure a permanent human presence there. The vastness of the territory plays a fundamental role here. It is therefore necessary to decide what to control and what is subsidiary.

The history of naval strategic thinking has thus been marked by the need to defend specific lines of communication or areas, with the possibility of carrying out occasional offensive actions to mark one's superiority. At the end of the 19th and beginning of the 20th centuries, A. Mahan, like J. Corbett, advocated a vision of naval superiority based on the control of communication lines, as well as on military force in support of these lines. In a certain sense – besides in a very historical perspective if we take up Mahan's work again –, the sea is seen as a network whose nodes and major lines must be protected. As for cyberspace, it is also based on this network logic, particularly in the physical layer, which must be dominated in order to have techno-industrial superiority. The 21st century major powers understand this well. The confrontation between the United States and China in cyberspace probably would not be the same without this struggle for network technology, illustrated in 2019 by the thorny issue of 5G acceptance, proposed by the Chinese company Huawei. It is a widely dividing issue, even within NATO countries. However, there is a major difference at this stage between the “natural” (or almost natural) nature of the maritime network and the “artificial” nature of the cyber network.
The issue of the law of armed conflicts also arises in the case of the integration of cyber in the maritime environment. If we consider the legal and ethical debates surrounding autonomous systems, armed or not, it is interesting to consider the latter in the maritime world. One of the main obstacles to the use of these systems in a military context comes from the sheer difficulty, even for humans, in discriminating between combatants and non-combatants in contemporary conflicts. This problem, which is particularly prevalent on land, is much less important underwater, where most of objects and men are from the military. It is therefore highly probable that the submarine domain will be the first to host autonomous systems, possibly armed, if only for experimental purposes. Indeed, the variety of missions that can be entrusted to these systems (intelligence, subsurface combat, mine warfare, etc.) makes it possible to greatly increase the capabilities of a naval force – if not in terms of performance, at least in terms of permanence – thus making it possible to partially solve one of the major challenges of naval strategy.

Beyond this question of cyberspace within the naval strategy itself, it is also important to consider that cyberspace is largely based on submerged maritime territory. Indeed, the overwhelming majority of cyberspace communications pass through an ever-increasing number of subsea cables. Because of the ease in implementing these infrastructures, making it possible to have high data rates at reasonable costs, the sea has very quickly overtaken space as a transit territory for global communications. The strategic understanding of subsea cables, as infrastructures laid at the bottom of the sea along fixed routes, is as much a matter of logic as it is of pipelines. But it also is a naval vision, with the challenge of laying and protecting them. Nevertheless, the paradox of communication at sea means that while cyberspace is mainly based on the maritime domain, ships have access to this same cyberspace through space systems. This particularity induces a particular vision of the stakes of cyber conflict on or under the seas.

Naval cyber-warfare

With the progressive digitization of ships, naval cyber-combat tends to move from a logic of disruption, as in the cyber domain in general, to a logic of immobilization/sabotage. With highly automated military and civilian ships, the risks associated with the loss of a ship's information subsystems are becoming increasingly critical. With a ship connected in multiple ways, by several types of wireless protocols, it is theoretically possible to launch more pernicious targeted attacks.

Embedded cyber systems are more strategically oriented to the logic of operational technology (OT) than information technology (IT). Naval platforms are complex industrial objects, with a lifespan of decades, which must house cyber sensor/effector systems whose obsolescence is much faster. This leads to a technological paradox, well known in the industrial world, between the load-bearing structure, whose safety comes from its stability, and the control system, which is by nature always in evolution. The challenge of the cybersecurity of the embedded system must take into account this specific aspect, with frequent updates, complex with regard to connectivity at sea. In addition, the vision of the ship as a cyber-industrial entity also needs to be further developed with the foreseeable increase of cyber-appendages that will be the various air, marine and submarine drones. They will use wireless communication protocols among themselves or with the carrier-vessel, bringing it closer to a connected factory type 4.0[5].

Given the importance of wireless communications, but also of the use of electromagnetic spectrum (AIS, GPS, UHF, etc.) for data transmission, it is possible to consider a merger of the cyber and electronic warfare domains at the naval tactical level. Embedded electronic warfare capabilities, including at the level of unmanned systems, should in this context become significant in denying access to data transmission systems, offering superior command and control to those who have such capabilities. For many years, the US Navy has been fostering programs of airborne UAVs (X-47, ScanEagle, etc.) with modular payloads, paving the way for such types of electronic warfare systems in the fleets.

Autonomous civilian and military naval systems will be prime targets for cyber attackers. Indeed, their reliance on data, whether produced by their own sensors or received (GPS, AIS), makes them sensitive to sophisticated forms of jamming or deception. The planned introduction of artificial intelligence to assist in the control of the ship and the accomplishment of its missions also opens up opportunities for attack, since it too can be the subject of specific attacks (code injection, recognition schemes disruption, etc.).

Pirates and privateers: towards new threats

Beyond the traditional state actors of maritime conflict, other dangers threaten military or civilian ships *via* cyberspace and could change the threat perception. In recent years, the cyber domain has seen the emergence of categories of actors whose behavior reminds us of the history of naval conflicts. Pirates are well known to sailors, but so far, they have been limited by an asymmetry of means and objectives that gives regular forces the advantage. In cyberspace, in view of the rapid learning of sophisticated attack techniques and the potential gains, non-state malicious actors are multiplying. Cyber pirates who obey a financial logic – in this sense,

[5] The so-called factories of the future, or as they are called in German, "4.0" factories, make extensive use of data in managing operations, including through the use of multiple robots and cobots as sensors or effectors.

cybercriminals or cyber-mobs, depending on their level of organization – could be willing to attack merchant ships and hold them for ransom, given the sums at stake in global maritime logistics[6]. Even if they represent only a limited danger to military forces, their impact on the maritime world could be significant in the coming years if the stakes are not properly assessed.

More dangerous are cyber-privateers[7] who work for the benefit of a given country that outsources its actions, either to avoid detection or for lack of skills. Cyber-corsairs are used to limit the risk of retaliation if the origin of the attack is discovered. Paradoxically, this situation makes it possible to maintain both a high level of conflict in cyberspace and the fog of war through uncertainty about the real motives and identity of the attacker. A particularly dangerous hypothesis would be the emergence of groups specializing in attacks against maritime systems – or even against connected industrial systems more generally – renting their services to the highest bidder. In this case, cyberattacks on hot spots like the Strait of Hormuz, the Black Sea or the China Sea may increase, with a corresponding rise in maritime insecurity.

Remote control of a connected or autonomous vessel could cause significant or even critical damage. Large ships, bulk carriers or giant chemical tankers of more than 100,000 tons, loaded with potentially harmful or explosive substances or carrying thousands of passengers[8], represent objects whose inertia could be diverted from a distance and launched against the quays of a port. Stopping them would be a very perilous task. Cybersecurity is thus becoming an important issue in the maritime world, since the risks associated with the diversion of fixed maritime platforms such as oil rigs, or of mobile platforms such as container ships, are particularly high. Cyber could thus create particular threats in the field of maritime terrorism[9]. Given the magnitude of the risks, the challenge of securing connected maritime systems and objects is a critical issue.

***

Naval and cyber strategies have many similarities. First, of course, is the control of a space where omnipresence is by nature impossible, which implies considering it as a network with hubs, lines and nodes of importance. The question of capacity is also significant. Cyber and marine are thus based largely on the intersection between technology, whose share is preponderant, and the will of human stakeholders. In short, if cyberspace is the only artificial strategic domain, the presence of Man in the maritime space also takes on a form of artificial nature. This similarity between the naval and cyber domains makes it possible to identify a number of common points or shared challenges.

While cyber has been forced to integrate a sea-oriented vision – for example considering the subsea cables issue – the maritime sector has to further integrate the cyber domain into reflections on opportunities and, especially, threats. Strategic thinking must consider data collection and processing platforms, sensors and effectors, and communication systems in order

[6] There are precedents in this respect, as was the case with the port of Antwerp, where hacking allowed drug traffickers to hide their activities between 2011 and 2013 (« Comment Anvers a été piraté et s'en est sorti », *La Libre Belgique*, 25 October 2013).

[7] These categories are obviously porous. It is quite possible that a pirate working for profit one day may be called upon the next day by some other country to conduct attacks that have a geopolitical purpose.

[8] The Symphony of the Seas, launched in 2018, has more than 8,000 people on board.

[9] However, this vision remains prospective, as cyber-terrorism does not exist yet (N. Mazzucchi, « Le cyberterrorisme a l'épreuve de la réalité », *Cahiers de la sécurité et de la justice*, n° 35-36, 9 September 2016).

to best integrate cyber systems throughout the maritime domain. Beyond these very immediate issues, a whole complex value chain must be set in motion within the Navy and in shipping companies, since the digital transformation involves industrial externalities as well as human ones (skills, training). For example, the evolution of energy requirements to meet the consumption of data transmission and processing requires a profound rethinking of the architecture of the electrical system (storage, efficiency, production) of ships, leading to new challenges in naval architecture. Cyber-maritime is thus far from being limited to a “simple” communication issue.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643