KIMS Periscope
For God · For Nation · For Peace

제336호 2024년 1월 11일

수면 너머: 해양안보의 6가지 공간 영역

2000년대에 해양을 이해하는 새로운 패러다임으로서 해양안보에 대한 활발한 논의가 시작될 때 주요 관심사는 선박과 항만 보안이었다. 테러, 해적과 밀수가 가장 주목받는 의제들이었다.

그러나 해양안보는 점점 더 다양해지고 복잡해지고 있다. 오염, 불법 어업, 기후 변화와 같은 환경 문제들이 논의에 포함되었으며 최근에는 사이버 보안과 해양 에너지 및 해저 데이터 케이블 보호에 대한 우려들이 해양안보에 대한 이해를 심화시키고 있다.

이와 동시에 해양안보의 영역도 확장되어왔다. 오늘날의 해양안보는 다차원적인 공간 영역을 고려해야 한다. 해양안보는 해수면, 공중, 저궤도, 수중, 해저면과 사이버로 구성된 6가지의 공간적 영역을 아울러야 한다. 본 기고문은 6가지 영역을 검토하고 6차원의 해양안보는 무엇을 의미하며 특히 해저면에 대한 고려가 필요한 이유를 살펴본다.

University of Copenhagen
Professor
Christian Bueger

(1) 해수면: 선박과 항구

해양안보는 역사적으로 항구 및 정박지를 통한 육지와의 연결과 항로를 포함하는 해수면에 주목해왔다. 해양 활동의 대부분이 해수면에서 이루어진다는 것을 생각하면 놀라운 사실은 아니다. 따라서 선박들은 상업용 화물선, 어선, 해양작업지원선(OSV) 등의 종류를 불문하고 보호의 주요 대상이다.

극단주의 단체, 해적들이나 기타 범죄자들로 인한 항행의 자유와 상업적 유통에 대한 위협과 불법 어업에서 비롯되는 환경파괴와 경제적 피해는 종종 해양안보의 핵심 이슈로 주목받는다. 그러나 해수면은 공간적 차원의 하나에 불과하며 기술발전의 가속화로 다른 영역들의 전략적 중요성이 증가하고 있다.

(2) 공중: 무선 통신, 감시와 드론 공격

항공보안을 위한 구체적인 제도들이 마련되어 있기 때문에 공중 영역은 해양안보에 대한 논의에서 제외되는 경우가 많다. 하지만 공중 영역이 유엔 해양법 협약에 포함된 데에는 타당한 이유들이 존재한다. 공중을 통해 바다에 접근할 수 있기 때문인데 이처럼 도서지역, 선박이나 해양시설에 접근하기에 가장 효과적인 수단은 주로 항공기와 헬리콥터이다.

이는 악의적인 행위자들에게도 마찬가지이다. 로켓 추진체나 무인 항공기로 해상의 목표물들을 공격하거나 헬리콥터를 통해 선박들을 납치할 수 있다. 인도양 북서부에서 일어난 일련의 사건들은 이 위협의 잠재적인 규모를 보여준다. 2021년에 유조선 스트리트호는 드론 공격을 받았고 2023년에는 후티 반군이 헬리콥터를 이용해 선박을 납치했다. 공중 영역은 해양안보의 핵심적인 축이다. 항공기와 드론을 사용하여 보다 넓은 해양 영역을 감시하고 헬리콥터를 통해 사고에 더 신속하게 대응할 수 있다. 마지막으로 무선 통신은 여전히 해상에서 주요 통신 수단으로 사용되고 있다.

(3) 저궤도: 위성과 부유식 우주공항

지구 저궤도는 해수면으로부터 1,000km 이하의 공간으로 정의되며, 영구적인 시설설치가 가

능하고 별도의 법적 체계가 적용된다는 점에서 공중 영역과 차이점을 가지고 있다. 최근 우주안보에 대한 논의가 활발해지고 있지만 해양과의 연관성은 거의 고려되고 있지 않다. 위성은 항법, 특히 대형 선박들이 의무적으로 장착해야 하는 선박자동식별장치(AIS)에 필수적인 요소이며 차세대 초소형 위성은 선단 관리, 항법과 통신의 혁신을 일으킬 것으로 기대된다.

또한 위성 감시는 대부분의 해양영역인식 시스템의 근간을 이룬다. 전자기 방출량과 같은 감시 데이터들은 AIS를 보완하여 AIS 없이 운행하는 '다크 선박' 탐지를 가능하게 한다. 또한 미사일 발사로 인해 발생하는 우주 쓰레기는 선박들에게 피해를 줄 수 있으며 떠오르는 저궤도 접근 기술 중 하나인 부유식 우주공항은 바다에서 경제적인 비용으로 우주발사체의 발사를 가능하게 한다.

(4) 수중: 마약 잠수함과 잠수정

수면에서 해저면까지의 공간을 아우르는 수중 공간은 잠수함이 등장한 이래로 해양 전략과 해전의 중심을 차지했으며 냉전 이후 핵 억지력의 핵심 요소이기도 하다. 해당 영역에서의 민간 활동이 레크리에이션 다이빙에 한정되어 있고 수중 공간 접근에 필요한 기술적 요구사항들을 고려할 때 수중 공간은 종종 해양안보 논의에서 제외되고는 한다.

그러나 이는 장거리 및 심해 잠수 장비에 대한 민간의 접근성 증가와 최첨단 방위산업 없이도 더 쉽고 저렴한 잠수정 건조가 가능해지고 있다는 점을 간과하고 있다. 마약 밀수에 사용되는 '나르코 잠수함'의 증가는 범죄자들에 의한 수중 공간의 악용이 증가하고 있으며 극단주의자들 또한 기뢰나 수중 드론으로 해당 공간을 악용할 여지가 존재한다는 것을 의미한다.

(5) 해저면: 필수 에너지 및 통신 인프라

인류의 역사를 통틀어 해저는 폐기물의 투기장이자 창고였다. 많은 군함들이 해저에 가라앉았고 군축 과정에서 탄약이 버려지기도 했다. 이런 심해 유물 중 일부는 해양유산이 되기도 했지만 발트해의 불발탄과 같은 경우에는 환경과 안전항해에 대한 심각한 위험 요소로 여겨지고 있다. 해저면이 해양안보에 중요한 이유는 이뿐만이 아니다.

해저면은 수세대에 걸쳐 모래, 암석과 다이아몬드와 같은 광물이 채굴되어져 왔는데 최근 심해 채굴 계획들로 인해 이러한 개발이 가속화되고 있다. 이로 인해 자원 도난이나 환경 파괴에 대한 우려가 제기되고 있다. 특히 에너지와 글로벌 통신에 필수적인 인프라가 자리하고 있다는 점에서 해저면은 해양안보에 중요한 의미를 지닌다.

석유와 가스 시추 플랫폼이나 풍력 및 태양광 발전 플랫폼과 같은 해양구조물들은 해저면에 고정되어 있다. 원유와 가스 파이프라인과 해저 케이블은 육지로 에너지 자원을 운송하여 다국적 에너지 시장의 활성화를 가능하게 한다. 1850년대에 전신선으로 전세계가 연결된 이후 글로벌 통신은 해저면에 설치된 케이블들에 의존하고 있다. 오늘날의 전세계적인 광섬유 케이블 네트워크에 전적으로 의존하고 있는데 총 데이터의 최대 99퍼센트가 이 네트워크를 통해 이동한다. 최근 노르트스트림과 발트해 파이프라인 사건들은 해저 인프라의 취약성을 상기시켰고 해저 인프라 보호를 해양안보의 일부로 자리잡게 하였다.

(6) 사이버: 자동화, 디지털화와 항해

자동화, 디지털화와 원격 제어의 추세는 해양 분야에서도 뚜렷하게 나타나고 있다. 상업항들을 완전히 자동화되어 있으며 위성 통신과 수치해도는 항해의 필수적인 요소로 자리잡았다. 또한 해양시설물들은 원격으로 제어되는 것이 지금의 추세이다. 따라서 네트워크 작전, 통신, 통합운용, 감시정찰, 자율운행 체계와 같이 해양안보에 필요한 역량들도 동일하게 디지털 영역에 대한 의존도가 높아지고 있다.

디지털 종속성은 고의적인 공격뿐만 아니라 다른 영역에 대한 공격의 여파에 대한 취약성을 의미하기도 한다. 디지털 수단은 특히 몸값 요구, 절도, 밀수 또는 불법 환적과 같은 범죄를 조장하는 데 이용될 수 있다. 사건 보고서들에 따르면 해양 산업에 대한 공격과 은밀한 해양 활동을 위해 AIS 위치데이터를 도용하는 사례들이 증가하는 추세에 있다.

6D 해양안보 전략

따라서 해양을 단일한 공간으로 접근해서는 안 된다. 해양안보가 전개되고 있는 다양한 공간 영역들은 각기 다른 활동, 인프라, 경제 및 환경적 이해관계와 안보 문제들을 내포하고 있다. 6가지의 기본적인 공간 영역은 더 세분화될 수도 있다. 지구물리학적 측면에서 빙하, 천해와 습지를 고려하거나 각각 고유한 특성을 지닌 사이버와 궤도의 여러 층위를 구분하는 것도 가능하기 때문이다.

해양안보는 항상 도전이자 기회였다. 해양에 대한 우리의 높은 의존도를 다시 숙고하여 해양의 안보를 위한 정책들과 기관들을 통합하고 조정할 수 있는 것은 기회이다. 그러나 해양안보의 복잡성과 이러한 통합과 조정을 실제로 수행하는 것은 큰 도전과제이다.

지금까지 이러한 복잡성은 관련된 행위자의 수와 국가 및 민간 부문이 함께 협력해야 할 필요

성의 측면에서 논의되어 왔다. 공간적 관점에서 해양안보를 6가지 공간 영역에서 이해하는 것은 복잡성을 증가시킬 수도 있지만 한편으로는 해양안보에 대해 생각할 수 있는 새로운 시각을 제공하기도 한다. 감시정찰과 다영역 작전의 통합을 요구하기 때문이다.

더 나아가 해양안보의 빈틈을 파악하는데 도움이 되기도 한다. 그런 측면에서 해양 사이버안보가 집중적으로 논의되고 저궤도가 주목받기 시작했지만 해당 영역에 대한 의존도과 취약성을 고려한다면 해저면의 전략화 또한 필수적이다.

전략적 틈새로서의 해저 영역

해저면은 세 가지 측면에서 점점 더 중요한 영역이 되고 있다. 첫번째로, 기후변화에 대한 대응으로 친환경 에너지 전환이 요구되며 해저면의 활용이 가속화되고 있다. 해저에 설치된 케이블들은 친환경 에너지의 전송과 통합된 전력시장의 운용을 가능하게 한다. 예를 들어 해저 케이블은 현재 가장 저렴한 친환경 에너지인 해상 풍력 발전소를 육상 전력망에 연결하고, 태양 에너지를 장거리 운송할 수 있기 때문에 북아프리카의 태양광 발전소를 유럽 전력망과 이어주고 호주에서 생산된 전력을 동남아시아로 전송할 수 있다. 차세대 해저 수소 파이프라인과 해저면에 이산화탄소를 저장하는 기술도 현재 개발 중에 있다.

둘째, 디지털화는 멈추지 않고 더욱 가속화될 것이다. 근미래에도 해저의 광섬유 케이블들이 가장 효과적인 전송수단으로 활용될 것이라는 것을 고려한다면 해저면에 더 많은 케이블들이 설치될 것이다.

셋째, 해저에 매장되어 있는 방대한 자원들을 개발될 것이다. 현재 심해 채굴에 대한 논의는 주로 개발 전망과 그 영향에 대해 진행되고 있어 유전자원에 대한 관심이 부족한 편이다. 그런데 해저 생물들이 견디는 가혹한 환경조건을 고려한다면 이 생물들의 유전자는 새로운 치료법의 개발하는데 참고가 될 수 있다. 이에 2023년에 채택된 '국가관할권 이원지역 해양생물다양성 보전 및 지속가능이용 협정'을 통해 유전자원 사용을 위한 법적 프레임워크가 마련되었지만 안보적인 영향들은 고려되지 않았다.

흔히 해저는 달의 표면보다 적게 알려져 있다고 전해진다. 그만큼 이 영역에 대한 (잠수함 탐지를 제외한) 지식과 인식이 부족하다는 것이며 이 문제를 '해저맹'('subseablindness')이라고 부를 수 있을 것이다. 영국과 EU의 새로운 해양안보 전략들은 이미 이 문제를 인지하고 있으며 이미

해저면을 지도화하기 위한 세계적 캠페인(Seabed 2030)이 진행 중이다. 또한 나토와 프랑스, 이탈리아 등의 해군들도 해저 프로젝트에 착수하였다. 이러한 노력들은 그동안 전략적 틈새였던 해저면에 집중하여 향후 몇 년 내에 성과가 나타날 것으로 예상되지만 결국에는 그보다 더 광범위한 6차원의 해양안보 구상과의 통합이 필요할 것이다.

KIMS Periscope
For God · For Nation · For Peace

Beyond surface: The six spatial domains of maritime security

Christian Bueger

Professor ,

University of Copenhagen

When debates on maritime security as a new paradigm for understanding the oceans intensified in the 2000s, the main concerns were ship and port security. Terrorism, piracy and smuggling were the main issues driving the agenda.

Increasingly, the maritime security agenda has diversified and multiplied. Environmental concerns, such as pollution, illegal fishing and climate change adaptation were included in the debate. Most lately, cyber security concerns, and the protection of offshore energy and underwater data cables further enriched the understanding of maritime security.

Hardly noticed, over the course of this expansion, also the spaces that concern maritime security have widened. Today security at sea needs to consider a multi-dimensional spatial domain. Maritime security concerns six spatial dimensions: surface, airspace, low orbit, subsea, seabed and cyber. In this contribution I review the six domains, then reflect on what it implies to think maritime security in 6D and why in particular the seabed requires further attention.

(1) Surface: Ships and ports

The maritime surface, including sea lanes and the connection to land through ports and anchoring zones, is historically the main focus of maritime security. This is unsurprising, since the majority of maritime activities take place on the surface. Ships are the main object of protection, whether its is commercial marine transport, offshore supply vessels or fishing boats.

Threats to freedom of navigation and commercial circulation from extremist groups, pirates or other criminals, but also the environmental and economic destruction caused by illicit fishing activities are often seen as forming the heart of maritime security. The surface, however, constitutes only one spatial domain, and technological acceleration implies that other domains increasingly gain strategic importance.

(2) Airspace: radio, surveillance and drone attacks

The airspace is often excluded from marine security debates, since there are specific regimes in place for aviation security. However, there are reasons for why airspace was for instance included in the UN Convention on the Law of the Sea. The sea becomes accessible through airspace. Often planes and helicopters provide the most effective means of transport to island, ships or offshore installation.

This applies to malign actors as well. Rockets and uncrewed aerial vehicles might be used to attack maritime targets, and helicopters can be used to hijack vessels. Incident in the Northwestern Indian Ocean indicate the potential scale. In the region, in 2021 the MT Mercer Street was attacked by drones, while in 2023 Houthi forces hijacked a vessel using a helicopter. Airspace is key in the provision of maritime security too. Surveillance of larger maritime spaces takes place through planes and drones, and helicopters allow for more rapid response time to incidents. Finally, radio communication continues to be the main mean of communication at sea.

(3) Low earth orbit: Satellites and floating space ports

The low earth orbit, defined as the space below 1000 km from the surface, differs from airspace in that it allows for permanent installations and is governed by a different legal regime. Discussions on space security have recently intensified, with the links to the maritime hardly considered. Satellites, in particular through the Automated Identification system (AIS) – compulsory for large seagoing vessels –, are important for navigation; and a new generation of micro-satellites is set out to revolutionize the management of fleets, navigation and communication.

Satellite surveillance forms the backbone of the majority of maritime domain awareness systems. AIS is increasingly complemented through other surveillance data, such as electro magnetic emissions, allowing for the detection of dark vessels that operate without AIS. Moreover, space garbage, for instance from missile launches has the potential to damage marine vessels, and one of the emerging technologies for accessing low earth orbit is from the sea, with floating spaceports providing a new affordable way to launch rockets.

(4) Subsea: Narco-submarines and submersibles

The subsea, consisting of the space from the surface to seabed, is a concern of sea power strategy and warfare since the emergence of submarine war in the 1920s, and a key space within nuclear deterrence since the cold war. Given the limited amount of civilian activity in this domain –recreational diving –, and the technological demands of accessing the domain, the subsea is often excluded from maritime security debates.

This neglects that long range and deep-sea diving equipment are increasingly available on civilian markets and that submersible vessels have become easier and cheaper to manufacture without the need for a high-end defence industry. The rise of what is know as 'narco submarines' – submersibles used in narcotic smuggling operations – indicates that the subsea is increasingly exploited by criminals, and

that extremists have opportunity to do so as well, for instance, in using mines or underwater drones.

(5) Seabed: Critical energy and communication infrastructure

Throughout human history, the seabed has been a dumping ground and storage space. Military fleets have been sunk to the ground to make them inaccessible to enemies, and ammunitions have been dumped as part of disarmament. Some of such deep-sea artefacts have become part of the marine heritage, others, such as the unexploded ammunition in the Baltic Sea, are today seen as major hazards for navigation and the environment. This is not the only way that the seabed matters in maritime security.

The seabed has been mined for generations for sand, rocks, and minerals, such as diamonds, and a new wave of deep seabed mining initiatives accelerates this development. This raises questions of theft and environmental damage. Perhaps most importantly for maritime security, the seabed hosts vital infrastructure for energy and global communications.

Offshore energy platforms, extracting oil and gas, or wind and solar energy, are mounted to the seabed. Oil and gas pipelines, and underwater electricity cables transport energy to the land, but also enable transnational energy markets. Global communication depends on cables laid on the seabed since telegraphic wires connected the globe in the 1850s. Today's internet is full dependent on a global network of optic fibre cables, through which up to 99% of data travels. Intentional damages to the Nord Stream and Baltic Connector pipelines have led to raising awareness of the vulnerability of seabed infrastructure, and made their protection part of maritime security.

(6) Cyber: Automation, Digitalization and Navigation

The trend towards automation, digitalization and remote control is as vivid in the maritime domain as elsewhere. Commercial ports are fully automated environments, navigation increasingly dependents on digital charts and satellite communications, offshore installations are remotely controlled. Maritime security capabilities are equally increasingly dependent on the digital realm, whether it is through networked operations, communication, force integration, surveillance, autonomous vehicles, or other ways.

Digital dependencies imply vulnerabilities from deliberate attack as well as from spill over from attacks in other domains. Digital means can be also used to facilitate crimes, in particular ransom, theft, smuggling or illicit transhipment operations. Incident reports point to a growing number of attacks on the maritime industry, and attempts to spoof AIS position data to hide maritime activity.

Strategizing Maritime security in 6D

As this exposition documents, we should not approach the maritime as singular space. Maritime security

unfolds in differentiated spatial domains, each implying different activities, infrastructures, economic and environmental stakes and security concerns. The six basic spatial domains, without doubt, can be further refined, such as in geophysical terms considering ice, shallow waters and wetlands, or in distinguishing the multiple layers of the cyber domain and the orbit, which each have their unique properties.

Since its inception, maritime security has always been a challenge and an opportunity. It is an opportunity to reflect on our profound dependency on the sea and to integrate policies and coordinate agencies to provide security. The complexity of maritime security and how to carry out integration and coordination in practice is, however, a major challenge.

So far, this complexity has been discussed in terms of the number of actors involved, and the need for governmental agencies, civil society, states and the private sector to work concertedly. Thinking in spatial terms, appreciating the six spatial domains of maritime security, on the one hand, adds further complexity, but on the other also gives us new lenses through which to think maritime security. It calls for further integrating surveillance and cross-domain operations.

It also gives us a better sense where the gaps are. While maritime cyber security is intensively discussed, and the low earth orbit only an arising domain, further strategizing the seabed is a requirement, given the profound dependencies and vulnerabilities of this domain.

The seabed domain as a strategic gap

The seabed is an increasingly important domain given three trends: First, the green energy transition required to address climate change implies an accelerated use of the seabed. Electricity cables on the seabed enable transmission of green energy and integrated electricity markets. They for instance connect offshore wind farms -- the currently cheapest green energy -- to terrestrial grids; solar energy can be transported across larger -distances, connecting for instance North African solar farms to the European networks, or Australian production to Southeast Asia. A new generation of hydrogen pipelines laying on the ocean floor is also on the horizon, as are technologies for storing Co2 in the seabed.

Second, digitalization is not going to stop, but will further accelerate. Since in the near future underwater optic fibre cables will continue to be the most effective means of transmission, more and more cables will be laid on the ocean floor.

Thirdly, the seabed holds vast resources which will be exploited. While much current debate concerns the prospects and consequences of mining deep seabed minerals, far less attention has been given to the issue of genetic resources. Given the harsh conditions under which species survive on the seabed, their genetic codes may offer paths to new therapies. The recent conclusion of the UN treaty on areas beyond national jurisdiction in 2023 provides a legal framework for genetic resources, yet without considering security implications.

It is often said that we know less about the seabed then the surface of the moon. Whether accurate or

not, it points to the lack of knowledge and awareness (beyond submarine detection) -- a problem that we might call 'subseablindness'. New maritime security strategies, for instance, by the UK and the EU already point to the problem, a global campaign is underway to map the seabed (Seabed 2030), and NATO and navies such as France and Italy have launched dedicated seabed projects. These are important initiatives to address the gap, with results expected in the coming years, which have to be, however, integrated in broader 6D maritime security architectures.

약력

Christian Bueger is Professor of International Relations at the University of Copenhagen, Denmark, where he leads the Ocean Infrastructure Research Group, and one of the directors of SafeSeas – the research network for maritime security and ocean governance. He is the author of *Understanding Maritime Security* forthcoming with Oxford University Press (with Tim Edmunds). Further information is available on his personal website: www.bueger.info

국내외 추천 참고자료

- Safeseas, "Critical Maritime Infrastructure Protection (CMIP)." 2023.
- European Union, "Maritime security: Council approves revised EU strategy and action plan" 2023.
- Christian Bueger $ Timothy Edmunds, " Maritime Security and the Wind. Threats and Risks to renewable energy infrastructures offshore", *Ocean Yearbook 38.* October 2023.

알림

- 본지에 실린 내용은 집필자 개인의 견해이며 본 연구소의 공식입장이 아닙니다.
- KIMS Periscope는 매월 1일, 11일, 21일에 구독자분들께 발송됩니다.
- KIMS Periscope는 안보, 외교 및 해양 분야의 현안 분석 및 전망을 제시합니다.
- KIMS Periscope는 기획 원고로 발행되어 자유기고를 받지 않고 있습니다.

웹페이지보기