For God · For Nation · For Peace
KIMS Periscope

제332호 2023년 11월 21일

사이버 전쟁과 해양 영역

무력분쟁에서 사이버 작전은 국제인도법(IHL)의 적용을 받는다. 디지털 인프라와 시스템에 대한 해양 영역의 높아진 의존도는 악의적인 사이버 작전에 취약하다. 그리고 이 취약점의 악용은 심각한 인도주의적 위기들을 초래할 수 있다. 항만, 정박소, 터미널과 같은 해양 인프라와 군사작전에 필요한 디지털 인프라도 사이버 작전의 목표가 될 수 있다. 그런데 분쟁 당사자는 특히 적대행위를 규제하는 국제인도법에 부합하는 수단과 방법만을 사용하여야 한다. 이는 사이버 작전도 마찬가지이며 국제인도법 상 군사적 목표의 개념과 구별, 비례성과 예방의 원칙들은 무력분쟁에서 국가들의 사이버 작전을 계속해서 규제한다. 사이버전이 해상전에서 점점 더 큰 역할을 할 것으로 예상되는 만큼, 국가들은 사이버 영역에서의 국제인도법이 어떻게 적용되는지 이해하기 위해 지속적으로 노력해야 한다. 국제적십자위원회(ICRC)는 국내, 국제적으로 해양 영역의 사이버 작전에 대한 국제인도법의 적용범위와 시기를 연구하고자 하는 국가들을 지원한다.

국제적십자위원회
해양법무전문관
(아시아태평양)
André Smit

국제적십자위원회
한국사무소 대표
Jamila Hammami

해상 영역에서 발생하는 악의적인 사이버 조치는 단순한 범죄부터 테러, 무력 분쟁 상황에서의 공격에 이르기까지 다양합니다. 무력 분쟁의 맥락에서 사이버 작전은 민간 선박에도 영향을 미칠 수 있으며, 무력 분쟁에서 사이버 작전의 사용은 국제 인도법(IHL)의 적용을 받는다.

해상 영역에서 발생하는 악의적인 사이버 활동은 단순 범죄부터 테러, 무력 분쟁에 이르기까지 다양하다. 무력분쟁에서 사이버 작전은 민간 해양운송에도 영향을 미칠 수 있으며 무력분쟁에서 사용되는 사이버 작전은 국제인도법의 적용을 받는다.

무력분쟁 중 사이버 작전은 민간인들에게 필수적인 인프라를 중단시킬 위험이 있으며, 이는 해상에서도 동일하게 적용된다. 군이 사용하는 민간 디지털 인프라는 무력분쟁 발생시 공격의 위험에 노출된다. 예를 들어, 사이버 공격으로 인한 민간 위성항법시스템의 중단은 해군뿐만 아니라 인도주의적 구호 활동에도 큰 영향을 미칠 수 있다. 또한 무인 해상 시스템과 같은 해상기반 민간 군용 플랫폼의 지속적인 디지털화로 인해 사이버 공격에 대한 취약성이 더욱 커지고 있다.

전세계 인구의 약 60%가 거주하고 있으며 미래의 경제 대국들이 위치하고 있는 아시아-태평양 지역은 긴장이 고조되고 있는 지역이기도 하다. IBM 보고서에 따르면 아시아-태평양 지역은 2022년에 2년 연속으로 가장 많은 사이버 공격을 받았던 지역이며 전세계적으로 수습된 사건들의 31 퍼센트를 차지했다. 민간인들과 통신에 필수적인 서비스를 제공하는 핵심 인프라에 대한 사이버 공격은 심각한 혼란을 초래할 수 있다. 역내에서 활동하거나 위치한 국가들은 사이버 역량을 보유하고 있으며, 공격 및 방어 목적으로 사이버 역량을 빠르게 발전시키고 있는 것으로 알려져 있다.

이러한 사이버 역량의 목표 중 하나가 민관군이 모두 활동하는 해양 영역이라고 생각하지 않

는 것은 안일한 생각이다. 국제인도법을 포함한 국제법은 다른 모든 영역과 마찬가지로 해양 영역에서 무력분쟁 당사자들의 행위 또한 규제한다. 19세기 이후 전쟁의 수단과 방법을 극적으로 변화했지만 싸우지 않고 적을 물리치는 오래된 전략은 새로운 디지털 수단을 활용한 전쟁 수행방식과 결합되고 있다.

디지털 수단을 통한 전쟁, 즉 사이버전은 모든 영역에서의 군사 작전을 계획하고 실행하는 사람들의 머릿속을 점점 더 채워가고 있다. 즉, 모든 영역이 사이버 영역과 연결되어 있는 것이다. 사이버 역량은 적의 사이버 역량에 영향을 미치거나 저하 또는 파괴하는 것; 센서, 무기 통제 기능 및 통신을 방해하거나 과부하를 일으켜 적의 눈을 '멀게' 하는 것; 스푸핑이나 디지털 수단을 통한 허위정보 확산을 통해 적을 기만하는 것; 디지털 인프라에 접근하여 적이 보고, 생각하고, 계획하고, 아는 것을 확인하는 것 등이 포함한다.

분쟁 당사자는 국제인도법과 특히 적대행위를 규제하는 규칙들을 준수하는 전쟁 수단과 방법만을 사용할 수 있다. 기존의 국제인도법은 이미 사이버 작전에 중요한 제한들을 가함으로써 강력한 법적 보호 방안들을 제공하고 있지만, 사이버 공간의 특성상 해석에 대한 어려움이 존재한다. 따라서 사이버 영역에서의 국제인도법 적용을 올바르게 이해하기 위해 국가들이 노력해야 할 필요성이 제기된다. 사이버전이 해상전에서 점점 더 큰 역할을 할 것으로 예상되는 만큼, 국가들은 해상을 포함한 무력분쟁에서 발생하는 사이버 작전을 규제하는 규정들에 대한 공동의 합의를 모색하고 교류를 지속해야 한다.

무력충돌 시 충돌 당사자들은 국제인도법에 의거하여 민간인과 전투원, 민간물자와 군사목표물을 구분할 의무가 있다. 해양 영역에서 사이버 작전의 잠재적인 목표에는 군함, 보조 함정, 군용 항공기와 해안 군사시설과 같은 군사목표물이 포함된다. 그런데 해상에서의 무력분쟁 시 민간 상선들도 나포 대상이 될 수 있으며 나포 과정에서 사이버전의 대상이 될 수 있다. 해양영역에서 적의 민간물자 사용이 국제인도법상 군사목표물의 정의를 충족한다는 엄격하게 정의되고 제한된 경우에도 사이버공격의 대상이 될 수 있지만, 이러한 사이버공격들은 여전히 적대행위를 규제하는 구별, 비례성과 예방의 원칙을 준수해야 한다.

민간 선박을 통한 해상운송이 국제인도법상 군사목표물로 분류될 수 있는 상황에서는 민간 선원들이 부수적인 피해를 입거나 직접적인 공격으로부터 보호를 받지 못하는 상황에 놓일 수 있다. 적의 전쟁수행 능력에 대한 직접적인 기여는 큰 위험을 수반하며 충돌 당사자의 전쟁수행 능력을 지원하도록 계약된 모든 상선은 물리적인 공격뿐만 아니라 사이버공격의 대상이 될 수 있다.

항만, 정박소, 터미널과 같은 관련 인프라와 상대의 군사작전 유지에 필요한 디지털 인프라도 사이버 작전의 대상이 될 수 있다. 선박들이 점점 더 디지털화되고 데이터화됨에 따라 사이버 작전은 안정성과 밸러스트 장치, 방향타와 엔진 등 선박의 안전한 항해에 필수적인 선내 다양한 시스템에 영향을 미치는 데도 사이버 작전이 사용될 수 있다.

선박의 항해능력 저하, 위성 위치 확인 시스템 (GPS) 또는 선박자동식별시스템(AIS)에 대한 전파방해나 스푸핑도 사이버 작전의 주목받고 있는 영역 중 하나이다. 선박을 다르게 보이게 하거나, 없는 곳에 있는 것처럼 보이게 하거나, 실제 있는 곳에 없는 것처럼 보이게 하는 것은 충돌 당사자에게 다양한 용도와 효용을 제공하고 상대방에게는 위험을 초래한다. 민간 해상운송의 불확실한 위치정보는 조난선박의 해상 항공 수색구조를 어렵게 하고 군이 해양에서 작전계획을 수립하며 의도한 군사작전구역 인근에 위치하고 있는 피보호자나 물자의 존재를 인지하지 못하게 된다. 부정확한 위치 식별 정보나 정보 위조로 인해 의도치 않게 민간물자가 공격 대상이 되어 손상되거나 파괴될 수 있는 것이다.

국제인도법상 사이버공격의 개념에 대한 더 명확한 정의가 필요하지만, 일반적으로 해상 영역을 포함하여 물리적 피해를 초래하는 사이버 작전은 국제인도법의 적용을 받는 공격에 해당하는 것으로 간주된다. 그러나 단순한 기능상실도 동일하게 해석될지에 대한 여부는 아직 결정되지 않았다. 민간인의 생존에 필수적인 물자와 같은 특정한 유형의 데이터는 국제인도법에 의해 보호된다. 현재에 같은 데이터 시대에서 필수적인 민간 데이터의 삭제나 변조가 국제인도법 위반이 아니라는 주장은 국제인도법의 목적과 취지에 부합한다고 보기 어렵다. 종이 문서와 자료가 데이터 형태의 디지털 파일로 대체되었다고 해서 국제인도법상의 보호범위를 벗어나는 것이 아니기 때문이다. 국제인도법의 보호범위에서 필수 민간 데이터를 제외하는 것은 치명적인 보호 공백의 발생으로 이어진다.

국제인도법상 공격으로 간주되는 사이버 작전으로 인해 해상 영역에서 발생하는 부수적인 민간인 피해를 감안한다면 합리적으로 예상할 수 있는 모든 직간접적 피해가 고려되어야 한다. 그 예로 사이버 작전의 직접적인 목표물은 아닐 수 있음에도 사이버전에 의해 야기되는 민간선박의 안전운항에 필요한 인프라와 시스템의 무력화가 있다. 국제인도법은 특히 구별, 비례성과 예방의 원칙이 성실하게 유지될 때 확실한 보호의 수단이 된다. 따라서 국제인도법은 해양 영역을 포함한 모든 무력분쟁에서 사용되는 합법적인 사이버 작전의 규제에 매우 중요한 역할을 한다.

이러한 배경에서 국제적십자위원회(ICRC)는 무력분쟁 시 사이버 작전의 한계에 대한 국제인

도법의 적용이 다양하게 해석될 수 있다는 점을 인지하고 있다. 따라서 사이버전이 야기하는 인도주의적 위기에 대응하기 위해서는 국가들, 특히 군과 사이버 전문가들과의 협력이 필수적이다. 무력분쟁 발생 시, 특히 해양에서 사이버전이 진행된다면 민간인들은 국제인도법 원칙에 따라 보호되어야 한다.

국제적십자위원회는 각 국가 및 군과의 대화와 토의를 통해 사이버 작전에 대한 한계를 식별하기 위해 활동하고 있다. 중립적이며 공평하고 독립적인 인도주의 기관으로서 국제적십자위원회는 국가들로부터 전쟁과 무력충돌로 인한 피해자들의 생명과 존엄성을 보호하는 임무를 부여받았다. 해양과 사이버 영역에서는 사이버 작전으로 인해 발생하는 민간 핵심기반시설과 민간인에 대한 추가적인 위험의 방지를 목표로 하고 있다. 국제적십자위원회는 이를 위해 대화와 교류에 전념하고 있으며 국내, 국제적으로 해양 영역에서의 사이버 작전에 대한 국제인도법의 적용범위와 시기를 연구하고자 하는 국가들의 노력을 지원한다.

Cyberwarfare and the Maritime Domain

ICRC Regional Resource Network, Asia Pacific

André Smit

Head of ICRC Mission in Seoul

Jamila Hammami

Malicious cyber measures encountered in the maritime domain range from simple criminality, through terrorism, to attacks in the context of armed conflicts. Cyber operations within the context of an armed conflict may also affect civilian shipping, and in an armed conflict, the employment of cyber operations is subject to international humanitarian law (IHL).

Cyber operations during armed conflict risk harming civilians by disrupting infrastructure and services essential to civilians, and this is equally applicable at sea. Armed forces often use civilian digital infrastructure, exposing them to risk of attack during armed conflicts. For example, civilian satellite navigation systems could be disrupted by cyber-attacks, causing major impacts not only to navies but also to relief operations of humanitarian workers. Moreover, with the continued digitization of civilian maritime- and military naval platforms - for example, the use of uncrewed maritime systems - create further vulnerabilities to cyber-attacks.

The wider Asia-Pacific, which is home to around 60% of the world's population and the future home of the world's largest economic powers, is also an area where tensions (including tensions in the maritime domain) proliferate. According to an IBM report, the Asia-Pacific region was the region that suffered under the most cyber 'attacks' in 2022 for the second consecutive year, accounting for 31% of all incidents remediated worldwide. Cyber operations against critical infrastructure enabling the delivery of essential services for the civilian population and telecommunications can result in serious disruptions. Many States in the region or operating therein have known cyber capabilities and are also known to be expanding this capability rapidly (both for offensive and defensive purposes).

There is no reason to think that this will not also focus on the maritime domain wherein the military and civilians operate, with the latter encompassing both government and private civilian components. International law, that includes IHL, regulates the conduct of Parties to armed conflicts in the maritime domain as it does in all other domains. Means and methods of warfare have changed dramatically since the 19th century but at the forefront of warfare, the 'age-old' strategy to defeat an enemy without firing a single 'shot' is married with warfare through newer digital means.

Warfare through digital means, or cyber warfare, is increasingly filling the minds of planners and executors of military operations in all domains, as all domains are linked to the cyber domain. Cyber capabilities include influencing, degrading, or destroying an enemy's cyber abilities; 'blinding' an enemy through jamming or overloading sensors, weapon direction capabilities and communications; deceiving an enemy through spoofing or disinformation fed through digital means; gaining access to digital infrastructure to see what enemies see, think, plan, know, and more.

A Party to a conflict may employ only such means and methods of warfare as would comply with the rules of IHL and specifically those regulating the conduct of hostilities. Existing IHL rules already offer strong protection by imposing important limits on cyber operations, but the nature of cyberspace poses challenges for interpretation. There is a need for States to work towards understanding how IHL applies in the cyber domain. Cyber warfare is expected to play an ever-increasing role in naval warfare, and States need to continue their exchanges and develop a common understanding on the rules that regulate cyber operations during armed conflicts, including those at sea.

During armed conflicts, IHL obliges belligerents to distinguish between the civilian population and combatants and between civilian objects and military objectives. The possible targets of cyber operations in the maritime domain could include military objectives such as warships, naval auxiliaries, military aircraft, and military naval coastal installations. It is possible that civilian merchant vessels may find themselves liable to capture during armed conflict at sea and as such they could be subjected to cyber measures in the process of effecting that capture. In the strictly defined and limited instances where the enemy's use of civilian objects in the maritime domain is such that they may fulfil the definition of a military objective within the meaning of IHL, they may be subjected to attacks through cyber operations too, although these cyber measures must be in accordance with the rules and principles governing the conduct of hostilities notably distinction, proportionality, and precautions.

In circumstances where the use of civilian sealift capability is such that it qualifies to be classified as a military objective within the meaning of IHL, it may put civilian operators and crews at risk of losing their protection from direct attack or they may be incidentally harmed. A direct contribution to an enemy's war fighting efforts would carry the most risk and it is to be expected that any merchant shipping contracted to support the war fighting efforts of a belligerent could become the subject of not only kinetic attack, but also cyber operations.

Associated infrastructure such as ports, roadsteads, and terminals and the digital infrastructure necessary to sustain an adversary's military operations may equally become the focus area of a belligerent's cyber activities. As vessels have become increasingly digitised and data-linked, a cyber operation may be used to affect systems of a ship that ensures its safe passage such as stability and ballast systems, the rudder and engines, and various systems on board that is relied upon for safe navigation and operation.

The degradation of a vessel's navigation capabilities or the jamming or spoofing of its Global Positioning System (GPS) or Automatic Identification Systems (AIS) is another area that has emerged as the object of cyber operations. To make a vessel seem what it is not, or be present where it is not, or to appear that it is not present where it actually is, has multiple possible applications and utilities for a belligerent and risks to an opposing belligerent. Uncertainty and degradation of the location data of civilian maritime shipping risks the inability of maritime and aeronautical search and rescue coordinators to assist a vessel in distress, while planners and executors of naval operations may not be aware of the presence of protected objects or persons in the vicinity of intended military operations. A civilian object may be inadvertently targeted, damaged, or destroyed as an unintended consequence due to the inaccuracy or falsification of location and identification information.

While more clarity is needed on the notion of attack under IHL in the context of cyber, it is generally agreed that cyber operations (also in the maritime domain) that result in physical damage would qualify as an attack that could trigger the application of IHL. Whether the mere loss of functionality would have similar effects remains to be determined. Certain types of data such as data related to objects indispensable to the survival of the civilian population are subject to specific protection under IHL. The assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the objective and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them. Excluding essential civilian data from the protection afforded by IHL to civilian objects would risk resulting in an important protection gap.

When considering incidental civilian harm in the maritime domain resulting from cyber operations that qualify as attacks under IHL, all reasonably foreseeable direct and indirect harm must be considered, including – for example – the degradation of infrastructure or systems required for continued safe civilian maritime operations for vessels, which is not directly and immediately caused by the cyber operation, but is nevertheless the product thereof. IHL affords strong protection provided that the rules and principles, notably that on distinction, proportionality, and precautions are applied in good faith. IHL is of critical importance in guiding lawful cyber-operations during armed conflicts including in the maritime domain.

Against this backdrop, the International Committee of the Red Cross (ICRC) is conscious that the exact limits that IHL imposes on cyber operations during armed conflicts remain subject to different views. Hence, collaboration with States, notably with military and cyber experts is crucial when it comes to addressing the humanitarian consequences posed by cyber means of warfare. If cyber capabilities are used in situations of armed conflict, notably in the maritime domain, civilians must remain protected by the principles of IHL.

The ICRC engages with States and militaries to allow a dialogue and raise questions to identify limits on cyber operations. As a neutral, impartial, and independent humanitarian organisation, the ICRC was mandated by the community of States to save lives and protect the dignity of people affected by armed conflicts. Considering the maritime domain, and cyber, it aims to ensure that cyber operations do not expose critical civilian infrastructure and civilian populations to additional harm. The ICRC is committed to dialogue and exchange of experience on these matters and perspectives on the matter. We also support States in their endeavour to further study - nationally and internationally - how and when IHL applies to cyber operations in the maritime domain.

약력

André Smit is the Regional Legal Adviser for Maritime Matters (Asia Pacific) at the International Committee of the Red Cross Regional Resource Network for Asia Pacific in Bangkok.
Jamila Hammami is the Head of Delegation of the International Committee of the Red Cross Delegation in Seoul.

국내외 추천 참고자료

- THE HINDU BUREAU, "IBM report says Asia-Pacific region faced the brunt of cyberattacks in 2022; manufacturing industry most targeted." *The Hindu.* February 22, 2023.
- Bart Hogeveen, The Future of Cyber Warfare in the Indo-Pacific", *ORF.* January 13, 2023.
- Laurent Gisel, Tilman Rodenhäuser, Knut Dörmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflictss" *The ICRC,* March 2021.

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