INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERATTACKS AGAINST CIVILIAN MARITIME INFRASTRUCTURE: ANALYZING THE THRESHOLD OF 'USE OF FORCE' AND 'ARMED ATTACK' UNDER UNCLOS AND THE JUS AD BELLUM FRAMEWORK

AUTHORED BY - AKANKSHA SINGH,
PhD Scholar Gujarat National Law University, Gandhinagar

CO-AUTHOR - FAHAD ABDULLAH,
PhD Scholar, Jamia Millia Islamia, Delhi

I. Executive Summary

The increasing digital dependence of global maritime activities has rendered civilian maritime infrastructure a critical yet vulnerable domain for cyber operations. This report examines the complex interplay of international law, specifically the United Nations Convention on the Law of the Sea (UNCLOS) and the *jus ad bellum* framework, in addressing cyberattacks on ships and ports. While existing legal principles are broadly applicable to cyberspace, significant ambiguities persist, particularly concerning the precise thresholds at which a cyberattack constitutes a 'use of force' or an 'armed attack'. The intangible nature of many cyber harms and challenges in attributing attacks to states complicate the application of traditional legal concepts.

The analysis underscores that a nuanced, effects-based approach is essential for classifying cyber incidents. However, this approach necessitates a deeper understanding of "harm" in the digital realm beyond physical destruction. The NotPetya cyberattack, which severely disrupted global shipping, illustrates these challenges. The "digitalization paradox," where progress brings new vulnerabilities, demands a shift in maritime security to integrate cyber-physical strategies and foster resilience. The difficulty in attributing cyberattacks allows malicious activities to operate in a legal "grey zone," undermining deterrence and necessitating enhanced international cooperation. The interconnectedness of civilian and military networks also challenges the application of International Humanitarian Law, particularly the principle of distinction, requiring urgent legal discourse on the nature of harm in the digital age.

ISSN: 2582-6433

II. Introduction: The Evolving Maritime Cyber Threat Landscape

The Increasing Digital Dependence and Vulnerability of Global Shipping and Port Infrastructure

Digitalization has revolutionized the global maritime industry and it is based on technologies, such as automated vessel management, IT networks, and the navigation systems of the vessels, such as AIS and GPS. This combination has increased efficiency but has exposed complex vulnerability to attacks on the field of cyber warfare.[1] The trend of attacks against essential operational technology (OT) and IT systems is incredibly frequent. An effective strike against one of the key ports is capable of causing the following ripples, resulting in the appalling economic effects and supply chain delays. As an example, a 2023 ransomware attack disabled more than 1,000 ships by going after a software vendor.[2] The concept of digitization, in which efficiency creates systemic brittleness, requires the paradigm of physical security to be replaced with cyber-physical tactics and an organizational system of cyber resilience.[3]

The meaning of Civilian Maritime Infrastructure in terms of the Cyber Threats

Critical maritime infrastructure refers to fundamental property, networks, and systems that are vital to the functions of societal activities, economic operations and safety. This involves commercial vessels, ports, control systems of operation as well as navigation systems and critical submarine cables. such infrastructures are subject to specific damage by armed conflict, sabotage, and complicated hybrid threats.[4]

The Unique Characteristics of Cyberattacks (Intangibility, Attribution Challenges, Non-Kinetic Effects)

Attacks on cyberspace are heavily different compared to the war. They are normally non-material and global in their scope. Although others result in direct kinetic effects, many will lead to indirect leakage, e.g. bringing automated systems to a halt or blinding radar, without any physical destruction.[5]

---

[1] Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures - Lex Portus, accessed June 20, 2025, https://lexportus.net.ua/vipusk-1-2025/melnyk_1111.pdf
[2] Maritime Ransomware | Blank Rome LLP, accessed February 9, 2025, https://www.blankrome.com/publications/maritime-ransomware
[3] Cybersecurity Framework for Maritime Port Management - Global Security Review, accessed May 15, 2025, https://globalsecurityreview.com/cybersecurity-framework-for-maritime-port-management/
[4] Protecting maritime infrastructure from hybrid threats: legal options - Hybrid CoE, accessed April 3, 2025, https://www.hybridcoe.fi/wp-content/uploads/2025/03/20250306-Hybrid-CoE-Research-Report-14-web.pdf
[5] The New Jurist | Cyber Warfare in International Law, accessed February 28, 2025, https://newjurist.com/cyber-warfare-in-international-law/

ISSN: 2582-6433

Tracing, or the identification of perpetrators of state-sponsored cyber attacks who are certain, is always a problem, because of the secrecy of cyber actions and the ability to operate through proxies or under false flags. The so-called attribution gap creates a strategic superiority of the aggressor: he not only is able to cause harm under the threshold of the use of weapons but uses plausible deniability to block the deterrent effect of international law.[6]

The question whether to comprehend non-kinetic consequences like functional loss or a serious violation of the economic sphere as an event classified as a breach of the international law or not is the most significant debate on classifying a cyberattack. This growing interdependence (in both military and civil networks, such as undersea cables and dual-use ports) raises serious concerns to the applicability of International Humanitarian Law (IHL) including the principle of distinction.[7] Cascading effects may result in a disproportionate civilian harm in an event of an attack on a target that is military in nature. This requires an immediate ethical and legal discussion to use such principles as proportionality to reflect the effects of digital disruption that are complicated.[8]

III. Foundational Principles of International Law: UNCLOS and Jus ad Bellum

A. UNCLOS: A Framework for Ocean Governance

Core Principles: Sovereignty over Internal/Territorial Waters, Innocent Passage, Freedom of Navigation in EEZ/High Seas

The United Nations Convention on the Law of the Sea (UNCLOS) establishes the legal framework for all maritime activities. In **internal waters**, the coastal state exercises absolute sovereignty. In the **territorial sea**, extending up to 12 nautical miles, the state also has sovereignty, but foreign vessels have the right of "innocent passage." This passage must be "expeditious and continuous" and not "prejudicial to the peace, good order, or the security" of the coastal state.[9] UNCLOS Article 19(2) lists non-innocent activities, including the threat or

[6] Attribution - International cyber law: interactive toolkit, accessed May 2, 2025, https://cyberlaw.ccdcoe.org/wiki/Attribution

[7] Sabotage of Submarine Cables and Pipelines as a Use of Force and Armed Attack - U.S. Naval War College Digital Commons, accessed June 25, 2025, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3105&context=ils

[8] Full article: Proportionality in cyberwar and just war theory - Taylor & Francis Online, accessed June 1, 2025, https://www.tandfonline.com/doi/full/10.1080/16544951.2023.2179244

[9] Cybersecurity in the Marine Transportation System - Federal Register, accessed May 12, 2025, https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-

ISSN: 2582-6433

use of force. Beyond the territorial sea, the **Exclusive Economic Zone (EEZ)** and the **high seas** are governed by the principle of freedom of navigation.[10]

Application of UNCLOS to Cyber Activities Affecting Maritime Spaces

UNCLOS principles, though pre-digital, extend to cyber activities. A state-sponsored cyberattack on a ship on the high seas or in an EEZ would infringe upon the flag state's freedom of navigation (Article 87(1)(a) or 58(1)), constituting an internationally wrongful act. Within the territorial sea, cyber activities inconsistent with innocent passage, such as cyber espionage, would be wrongful, allowing the coastal state to take countermeasures.[11]

UNCLOS also addresses piracy (Article 101), defined as illegal acts of violence for private ends. While traditional interpretations require two ships, some argue it could encompass depredations against submarine cables by non-state actors.[12] Cyberattacks that interfere with navigation systems to alter routes, cause collisions, or enable theft threaten maritime safety and could violate UNCLOS principles of safe navigation and state responsibility.[13]

The application of UNCLOS's foundational principles to cyber activities shows it is a "living instrument" capable of evolving. However, the lack of explicit cyber rules creates ambiguity, as states must rely on broad interpretations, potentially leading to disputes. This underscores the need for states to clarify their positions and consider new protocols to enhance stability in the maritime cyber domain.

The "Peaceful Uses of the Oceans" Principle and its Relevance to Cyber Operations

UNCLOS proclaims the fundamental need for the peaceful use of the oceans. Article 301 obliges states to "refrain from any threat or use of force against the territorial integrity or political independence of any State."[14] This prohibition extends to cyber operations that disrupt

system

[10] Peacetime use of Force, Military Activities, and the New Law of the Sea, accessed May 10, 2025, https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1152&context=cilj

[11] Cyberwarfare and International Law - UNIDIR, accessed March 18, 2025, https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf

[12] Attacks on Submarine Cables and Pipelines: A Self-Defence Approach Complementary to Law Enforcement - EJIL: Talk!, accessed June 28, 2025, https://www.ejiltalk.org/attacks-on-submarine-cables-and-pipelines-a-self-defence-approach-complementary-to-law-enforcement/

[13] Piracy and Undersea Cables: An Overlooked Interpretation of UNCLOS? - EJIL: Talk!, accessed June 10, 2025, https://www.ejiltalk.org/piracy-and-undersea-cables-an-overlooked-interpretation-of-unclos/

[14] Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum Michael N. Schmitt, accessed February 5, 2025, https://harvardnsj.org/wp-content/uploads/2017/02/Schmitt-NSJ-Vol-8.pdf

ISSN: 2582-6433

maritime activities. Such operations, if they reach a sufficient severity, could violate the peaceful uses principle, even without kinetic means.[15]

B. Jus ad Bellum: The Prohibition on the Use of Force

Article 2(4) of the UN Charter: General Prohibition on the Use or Threat of Force

Jus ad bellum governs when states may lawfully resort to force. Its cornerstone is Article 2(4) of the UN Charter, which prohibits the threat or use of force in international relations. This prohibition is also part of customary international law.[16]

Article 51 of the UN Charter: The Inherent Right to Self-Defense Against an 'Armed Attack'

The primary exception to this prohibition is the inherent right of self-defense under Article 51, which may be exercised "if an armed attack occurs." The International Court of Justice (ICJ) confirmed this right applies to any use of force, "regardless of the weapons employed," including cyber means. For self-defense to be lawful, it must be both necessary and proportionate to repel the attack.[17]

Distinction Between 'Use of Force' and 'Armed Attack' (Gravity Threshold)

Not every 'use of force' is an 'armed attack'. An action must reach a "certain degree of gravity" to trigger the right of self-defense. The ICJ, in the *Nicaragua* case, distinguished between "the most grave forms of the use of force" (armed attacks) and "other less grave forms." This "scale and effects" standard is central to assessing cyber operations. However, there is no international consensus on the precise threshold, and many state-sponsored cyber operations are assessed to fall below it.[18]

The prevailing "effects-based" approach classifies a cyberattack based on its consequences rather than the means employed. While this offers a flexible way to apply existing law, it struggles with non-kinetic effects. Quantifying the "gravity" of economic disruption or data loss compared to physical destruction remains a significant challenge, perpetuating ambiguity

[15] Cyber Attacks and the Use of Force in International Law - Helda - University of Helsinki, accessed May 22, 2025, https://helda.helsinki.fi/bitstreams/9d3f583f-314b-4f89-978c-c4676002c446/download
[16] Use of force - Rulac, accessed May 28, 2025, https://www.rulac.org/legal-framework/use-of-force
[17] Use of Force in Cyberspace | Congress.gov, accessed April 20, 2025, https://www.congress.gov/crs-product/IF11995
[18] Attack (international humanitarian law) - Cyber Law Toolkit - CCDCOE, accessed June 30, 2025, https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law

ISSN: 2582-6433

without a clearer, shared understanding of "harm" in the digital age.[19]

IV. Cyberattacks as 'Use of Force' and 'Armed Attack': A Jurisprudential Analysis

A. The "Scale and Effects" Test

The ICJ's "scale and effects" criteria from the *Nicaragua* judgment is widely applied to cyber operations.[20] Cyber operations causing physical damage, injury, or death are unambiguously considered 'uses of force'. To be an 'armed attack' triggering self-defense, the consequences must be "sufficiently grave," comparable to a conventional armed attack, implying widespread fatalities or severe destruction.[21]

B. The Debate on Non-Kinetic Harm

The classification of non-kinetic harm is highly contentious. While some, like the ICRC, interpret "attack" to include loss of functionality without physical damage, others, like Denmark, maintain that only physical damage is relevant.

Historically, Article 2(4) was not seen as encompassing economic coercion. However, cyber operations capable of inflicting severe economic consequences may necessitate a reappraisal of this issue. There is currently no consensus on whether non-kinetic attacks crippling financial institutions or government services constitute an 'unlawful use of force' or an 'armed attack'. This challenges the traditional "analogy-approach" to cyber warfare, which focuses on physical destruction. It overlooks the novelty of cyberattacks that are disruptive rather than destructive but still pose severe threats to digitally dependent societies.[22]

C. Thresholds in Practice

No such precedent of a state declaring a cyber operation a use of force or armed attack has

[19] The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack (Chapter 6) - Cyber Operations and International Law - Cambridge University Press, accessed May 30, 2025, https://www.cambridge.org/core/books/cyber-operations-and-international-law/threshold-of-cyber-warfare-from-use-of-cyber-force-to-cyber-armed-attack/18EED20277D22CAE25E71F63A27C8009

[20] Cyber Attacks as "Force" Under UN Charter Article 2(4) - Scholarship Archive, accessed March 22, 2025, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1882&context=faculty_scholarship

[21] International Responsibility for the Unlawful Use of Force: States, Organizations, Armed Groups and Individuals (Chapter 15), accessed April 8, 2025, https://www.cambridge.org/core/books/use-of-force-and-the-international-legal-system/international-responsibility-for-the-unlawful-use-of-force-states-organizations-armed-groups-and-individuals/CA4F717393B885BB60AE719B16FD6383

[22] Technology - Shippers get serious about cyber threat - Allianz Commercial, accessed June 15, 2025, https://commercial.allianz.com/news-and-insights/expert-risk-articles/shippers-cyber-threat.html

ISSN: 2582-6433

occurred so far which suggests that these events have not reached lines of recognition addressed by the international law. One of the primary non-binding documents is the Tallinn Manual 2.0, which also contains guidance, arguing that the standard of "use of force" is satisfied when the effect of a cyber operation is functionally equivalent to that which an operation involving non-cyber use of force causes. [23] The attack must be a higher level of severity to be termed as an armed attack. Moreover, the Manual determines that cyber espionage is not, as a rule, a contravention of international law, but the methods used in it may be illegal. [24]

Table 1: Comparative Analysis of 'Use of Force' vs. 'Armed Attack' in Cyber Operations

Criterion	'Use of Force' (UN Charter Art. 2(4))	'Armed Attack' (UN Charter Art. 51)
Legal Basis	General prohibition; Customary International Law.	Exception to prohibition; Right to self-defense; Customary International Law.
Threshold	Broadest and lowest threshold.	Graver form of use of force; Triggers right of self-defense.[25]
Defining Element	Action coercing or impacting territorial integrity/political independence.	The "most grave forms of the use of force".
Key Test	"Scale and effects" comparable to non-cyber uses of force.	"Scale and effects" reaching a certain severity.
Nature of Harm (in Cyber Context)	**Clear Cases:** Physical destruction, death, injury. **Debated Cases:** Significant loss of functionality, severe economic disruption.	**Clear Cases:** Widespread fatalities, destruction comparable to conventional attack. **Debated Cases:** Fundamental compromise of state function; irreversible societal disruption.
Examples in Cyber Context	Temporary incapacitation of critical infrastructure, widespread	Widespread, sustained power outages causing deaths; destruction of critical

[23] The use of force (Chapter 14) - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - Cambridge University Press, accessed March 5, 2025, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/use-of-force/F2871424CF6758F2C9275568B777DF51
[24] Tallinn Manual 2.0: Cyber Espionage Generally Not Unlawful - CCDCOE, accessed April 6, 2025, https://ccdcoe.org/news/2017/tallinn-manual-2-0-cyber-espionage-generally-not-unlawful/
[25] The Tallinn Manual - CCDCOE, accessed February 17, 2025, https://ccdcoe.org/research/tallinn-manual/

ISSN: 2582-6433

Criterion	'Use of Force' (UN Charter Art. 2(4))	'Armed Attack' (UN Charter Art. 51)
	but reversible data corruption.	infrastructure (dams, nuclear plants).[26]
Legal Consequences	Internationally wrongful act; State responsibility; Permissible non-forcible countermeasures.	Right to self-defense (may include force); Reporting obligation to UN Security Council.
Attribution Requirement	Necessary to invoke state responsibility.	Necessary to justify forceful self-defense.
Consensus Level	Low and evolving for cyber; significant disagreement on non-kinetic effects.	Even lower consensus; high bar for non-kinetic effects.

V. The Challenge of Attribution and State Responsibility in Cyberspace

Difficulties in Identifying Perpetrators and Linking Cyberattacks to States

Attribution is a prerequisite for invoking state responsibility. While public political attributions have increased, the evidence to prove them is rarely provided publicly. Adversaries use sophisticated techniques like proxies and "false flags" to obscure their origins, making it difficult to present the clear evidence needed to justify retaliation under international law.[27]

This "attribution gap" is a strategic advantage for aggressors, allowing them to inflict harm below the threshold of armed conflict while maintaining plausible deniability. The absence of an obligation to publicly provide evidence undermines the deterrent effect of international law, as victim states struggle to justify legal responses like countermeasures or self-defense.

International Law Commission's Articles on State Responsibility (ARSIWA) and their Application to Cyber Attribution

There is a broad consensus that the general rules of state responsibility, particularly ARSIWA,

[26] The unintended consequences of deterring cyber attacks through nuclear weapons and international law | European Leadership Network, accessed February 10, 2025, https://europeanleadershipnetwork.org/commentary/the-unintended-consequences-of-deterring-cyber-attacks-through-nuclear-weapons-and-international-law/

[27] Attributing cyber operations under International law: Political and legal aspects - QIL QDI, accessed June 7, 2025, https://www.qil-qdi.org/attributing-cyber-operations-under-international-law-political-and-legal-aspects/

ISSN: 2582-6433

apply to the cyber context.[28] Under ARSIWA, a state is responsible for the conduct of its organs (Article 4). The conduct of non-state actors is generally not attributable, except under specific circumstances, such as when the actor is "acting on the instructions of, or under the direction or control of, that State" (Article 8).

While ARSIWA provides a necessary legal framework, applying concepts like "direction or control" to sophisticated non-state cyber actors places an interpretive strain on these rules and creates a high evidentiary bar. This highlights the practical challenges of applying existing legal frameworks and raises questions about the "due diligence" obligation of states to prevent their territory from being used for attacks.

Implications of Attribution for Invoking State Responsibility and the Right to Self-Defense

Reliable attribution is essential for a victim state to invoke state responsibility, enabling countermeasures or, in grave cases, the right to self-defense. When a state considers a response, the standard of attribution is generally "reasonableness." Non-state actor operations at the 'armed attack' level are legally challenging, but most experts believe they can qualify as armed attacks, potentially allowing a forceful response, especially if a state is "substantially involved."

VI. Case Study: Not Petya and its Maritime Implications

A. Overview of the NotPetya Attack

The NotPetya malware of June 2017[29] was a destructive wiper disguised as ransomware, designed for disruption, not financial gain. Initially targeting Ukrainian organizations on the eve of Ukraine's Constitution Day, it suggests an intent to undermine state functions. The attack caused global economic losses estimated in the billions.[30]

The maritime sector was severely impacted. Shipping giant A.P. Møller–Maersk was forced to suspend global operations, reinstall 4,000 servers and 45,000 computers, and suffered losses exceeding $300 million. The incident highlighted the interconnectivity of global shipping,

[28] The Application of International Law to State Cyberattacks - Chatham House, accessed May 5, 2025, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf
[29] A Closer Look at NotPetya - Portnox, accessed April 2, 2025, https://www.portnox.com/cybersecurity-101/notpetya-attack/
[30] International Humanitarian Law and the Targeting of Data - U.S. Naval War College Digital Commons, accessed June 12, 2025, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1725&context=ils

ISSN: 2582-6433

showing how one company's failure could cascade across the sector. Several nations, including the US and UK, formally attributed the attack to state-sponsored actors linked to the Russian government, based on technical and geopolitical analysis. This attribution reclassifies the incident from a cybercrime to a state-sponsored cyberattack, which has direct implications under international law.[31]

B. Legal Analysis through the Lens of Jus ad Bellum and UNCLOS

Application of 'Use of Force' and 'Armed Attack' Thresholds

The NotPetya attack is a compelling case for applying *jus ad bellum* thresholds to cyber operations. While not a kinetic attack, its "scale and effects"—paralyzing a global shipping company and causing massive economic loss—were severe. The wiper's destructive intent supports its classification as a hostile act. Under an effects-based approach, the operational paralysis and severe economic disruption could constitute a 'use of force' under UN Charter Article 2(4).

It remains legally uncertain whether the incident was severe enough to qualify as an 'armed attack' under Article 51, the standard required to justify a response in self-defense. While some scholars argue severe economic consequences can qualify, the lack of direct fatalities or widespread physical damage makes this classification challenging under restrictive interpretations.[32]

Attribution Challenges in the NotPetya Context

Despite public attribution to Russia, the attack highlighted the "attribution gap." The use of sophisticated masking techniques complicated legally certain attribution required for invoking state responsibility. This gap allows states to conduct disruptive operations with plausible deniability, complicating an international legal response.

[31] Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield, accessed April 25, 2025, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1198&context=dltr

[32] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, accessed March 10, 2025, https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N.*Schmitt-Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017*.pdf

ISSN: 2582-6433

Implications for UNCLOS Principles (e.g., Freedom of Navigation, Peaceful Uses)

By crippling Maersk, NotPetya impeded the freedom of navigation for its fleet and undermined the "peaceful uses of the oceans" principle enshrined in UNCLOS.[33] The incident demonstrated that cyber operations can effectively paralyze maritime commerce, achieving disruptive effects comparable to a physical blockade and showing that threats to maritime security now include intangible cyber means.[34]

Philosophical Implications: Redefining Harm and Aggression

NotPetya is a prime example of non-kinetic, disruptive harm that compels a re-evaluation of legal definitions of aggression. It caused immense operational chaos and billions in losses without widespread physical destruction. This challenges the "analogy approach" to cyber warfare, which ties regulation to kinetic effects. NotPetya showed that aggression can be decoupled from physical violence by targeting data and software to cripple societies.[35] This necessitates a broader understanding of "harm" that includes severe functional impairment and economic paralysis.[36]

VII. Evolving International Law and Future Considerations

A. Current Gaps and Ambiguities

Significant gaps persist in applying international law to cyberspace. There is no consensus on the thresholds for non-kinetic cyber harm to qualify as a 'use of force' or 'armed attack'. [37]This creates a "grey zone" where states can inflict substantial damage without clear legal repercussions, eroding international stability. The deep integration of civilian and military networks also challenges the application of IHL principles like distinction and proportionality.[38]

[33] Maritime Cyber Security Regulations - DNV, accessed March 28, 2025, https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/

[34] Many valuable lessons in UNCLOS for international governance of cyberspace | UNCLOSdebate.org, accessed June 18, 2025, https://www.unclosdebate.org/argument/1231/many-valuable-lessons-unclos-international-governance-cyberspace

[35] From Theory to Practice Developing a National Position on International Law in Cyberspace, accessed June 5, 2025, https://www.youtube.com/watch?v=_o93N97jhG0

[36] Why we need philosophy and ethics of cyber warfare | University of Oxford, accessed April 10, 2025, https://www.ox.ac.uk/news/2022-06-16-why-we-need-philosophy-and-ethics-cyber-warfare

[37] Handbook on maritime hybrid threats: 15 scenarios and legal scans, accessed April 15, 2025, https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf

[38] Reinterpreting the legality of forcible self-defence in response to non-kinetic cyber attacks - Melbourne Law School, accessed February 20, 2025, https://law.unimelb.edu.au/__data/assets/pdf_file/0007/5068537/Hines-Advance-Copy.pdf

ISSN: 2582-6433

B. Emerging Norms and Initiatives

In response, various initiatives are emerging. The International Maritime Organization (IMO) has issued guidelines (MSC.428(98)) for cyber risk management.[39] National regulations, like those from the U.S. Coast Guard and the EU's NIS2 Directive, are establishing minimum cybersecurity requirements for vessels and ports. The Tallinn Manual continues to be a crucial scholarly resource fostering legal clarity. These efforts contribute to developing state practice and future customary law.

C. Philosophical and Jurisprudential Directions

Cyberattacks suggest reconsidering concepts of law. [40]The definition of harm must be broadened to cover functional and economic paralysis as an urgent necessity. This implies the rejection of the so-called analogy- approach and the acknowledgement of the fact that cyberattacks dis-integrate aggression and violence but are capable of destroying societies. New theories, including substantive necessity argument, have been advanced, suggesting that an example of a non-kinetic attack would constitute an act of armed attack in the event it involves the significant degradation of infrastructure critical to the capacity of a state to operate.

VIII. Conclusion

The attack of the civilian maritime infrastructure by cyber means puts the conventional legal provisions such as UNCLOS and jus ad bellum to the test. Although basic principles may be used, major ambiguities are still present on the criteria involving the use of force or armed attacks in relation to cyber.

The scale and effects test is both practical and controversial as it is applied in non-kinetic harms such as economic disruption. This brings up one of the fundamental dilemmas: rethinking the notion of harm that goes beyond physical forms. This can be shown through the NotPetya incident, where one could not clearly assume that a devastating non-kinetic assault resulted in a subjective and objective right to forceful self-defence.[41]

[39] Maritime cyber risk, accessed June 22, 2025, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[40] The Ethics of Cyber Conflict - Faculty, accessed February 2, 2025, https://faculty.nps.edu/dedennin/publications/Ethics_of_Cyber_Conflict_%20from_The_Handbook_of_Information_and_Computer_Ethics.pdf

[41] International Legal Basis For The Right To Defense In The Cyber Era | Law and world, accessed February 14, 2025, https://lawandworld.ge/index.php/law/article/view/302

ISSN: 2582-6433

Even more law breaking is the issue of the so-called attribution gap, under which malign cyber-missions remain within a legal gray area, hindering deterrence. Finally, addressing state positions effectively, further developing international cooperation, and a philosophical deeper dive into the concept of digital harm are needed in order to make the much-needed stability in the maritime cyber environment available and sustainable.