AYONIZ MUN

AZMUN Foundation
International Youth and Policy Affairs Association
Liaison Office – Geneva, Switzerland
Registered Address (India):
Sy. No. 60, Huskur Village & Sy. No. 151, Bommenehalli Village,
Bidarahalli Hobli, Bengaluru, Karnataka 560049
Phone: +91 (810) 650-0777
Email: contact@azmun.org | Website: www.azmun.org

Strengthening Maritime Cybersecurity: The Role of Youth in Protecting Global Shipping

Overview

Global importance of maritime cybersecurity

Maritime transport remains as a powerful means of the world economy where roughly about 90 % of global trade moves by sea serves to protect ships, shipping infrastructure, and associated industries from cyber threats and attacks. This shows that any disruptions to shipping whether physical or digital can cause a chain reaction across supply chains, national economies, and vital infrastructure. The digital transformation within maritime systems such as navigation, shipboard sensors, fleet coordination, logistics platforms as well as port automation brings efficiency, but also introduces open vulnerabilities.

In past few years, the maritime sector has seen an raise in cyber incidents such as major shipping firms like Maersk, COSCO, MSC, and port operators have reported attacks like ransomware, malware infiltration that disrupted systems and affected the supply chains. Such an instance was NotPetya attack of 2017, Maersk's global operations were deeply impacted which required a full IT rebuild, the losses have been estimated in the hundreds of millions of dollars.

Additionally recently, geopolitical tensions have intensified cyber threats to the maritime domain. A Cyble report in 2025 has documented over a hundred attacks on individuals working in the maritime industry activities including GPS spoofing, VSAT disruptions, and coordinated campaigns targeting port and shipping infrastructure.

To regulate and manage approaches, the International Maritime Organization (IMO) adopted Resolution MSC.428(98) (effective January 2021) which requires cyber risk management be integrated into ship Safety Management Systems (SMSs). Recommends stakeholders adopt strict layered security, training, immediate incident response, and governance processes. However, gaps in capacity, regulatory alignment, and workforce readines remains an hurdle.

Why youth involvement matters

Young professionals students, early-career technologists, cybersecurity enthusiasts bring much more advantages than expected

Digital fluency and innovation mindset: As emerging and being in a generation of technological advancement they often tend to be more attuned to emerging technologies such as AI, machine learning, autonomous systems and may this may benefit in proposing technogical architectures or detection systems.

Fresh perspective and courage: Without the ingrained institutional bias, youth can freely question the legal practices, push for ideals and bold reforms or standardized frameworks.

Scalability and network effects: Skilled youth can propagate and widen best practices worldwide through universities, local ports, developing regions and using other means thus amplifying developed impact.

Yet, their potential remains relatively dormant in maritime cybersecurity. A purposeful policy push to integrate youth could expand the talent pipeline, aid innovation, and foster long-term resilience in global shipping.

2. Key Challenges Young People Face in Maritime Cybersecurity

While youth engagement offers promising revolution, there are certain structural and practical obstacles that remain as limitations to their contributions. Below are major challenges:

1. Lack of maritime-specific cybersecurity education and training:
Standard cybersecurity programs seldom cover operational technology (OT) in ships or ports, maritime protocols, AIS, navigation systems, or port control systems. Despite the sector's importance, maritime cybersecurity remains underexplored, leaving significant gaps in understanding its challenges and risks.

2. Limited entry pathways in a hierarchical sector.
The maritime sector traditionally privileges experience, certifications, or Nautical qualifications. Early-career or youth contributions may be inderserved, and access to internships or project roles in ports or shipping companies is often limited.

3. Weak mentorship, networking, and institutional bridges
Young individuals creating connections to maritime regulators, port authorities, classification societies, and cybersecurity firms. This creates a gap between technical ideas and standardization within institutions.

4. Resource and infrastructure constraints in many countries.

In developing regions, digital infrastructure, funding for labs or Interactive learning environments, reliable connectivity, and scholarship support are limited. This worsens the inequality in youth capacity across geographies.

5. Fragmented regulatory frameworks and unclear youth roles

Variations in national adoption of IMO guidelines, differing cybersecurity standards (NIST, IEC, ISO) across states and operators, and uncertainty over reporting thresholds dissuade proactive youth-driven engagement.

3. Examples of Youth-Led or Youth-oriented Initiatives Globally

Cyber-SHIP Lab (University of Plymouth, UK)

A research lab hosting graduate and undergraduate researchers, the Cyber-SHIP Lab builds simulation environments, stress tests maritime networks, and collaborates with industry to find a weakness in an information system, software, hardware, or organizational process that allows a malicious actor to cause harm, gain unauthorized access, or disrupt services. This lab environment functions as an creates a controlled environment for young technologists to engage with real maritime cyber challenges.

Maritime Cybersecurity Roundtable and Industry MoU, Singapore

Singapore's Maritime and Port Authority (MPA) launched a Maritime Cybersecurity Roundtable and signed a Memorandum of Understanding with industry, academic institutions, and youth institutions to create training curriculum, simulation labs, and career pathways for youth in maritime cybersecurity.

Kenya's Youth Dialogue on Maritime Careers

As part of IMO's GreenVoyage 2050 outreach, Kenyan youth forums have included maritime cybersecurity among priority topics. The need for scholarships, mentorships, and visibility of maritime careers in STEM outreach had been put up.

4. Actionable Policy Recommendations to Boost Youth Participation

4.1 Establish a Global Maritime Cyber Fellowship / Youth Incubator Program

Design & funding: An annual competitive fellowship targeting students and young professionals , supported jointly by IMO, World Bank, regional development banks, and private shipping cybersecurity firms.
Structure: By Combining coursework, cross-national placements mentorship by senior maritime cybersecurity professionals, and project-based deliverables e.g. port vulnerability assessments, design of incident-response tools.
Outcomes: Fellowships give rise to tangible open source tools, policy briefs.

4.2 Maritime-Focused Cybersecurity Modules in Higher Education:

Curriculum standards: Regulatory bodies e.g. national maritime authorities should require or incentivize inclusion of maritime cyber modules like shipboard OT, navigation security, port ICS/SCADA within engineering, maritime, and cybersecurity degree programs.
Grants and seed funding: Offer grants to universities (especially in developing countries) to develop labs, simulation infrastructure, and faculty capacity.

4.3 Institutionalize a Youth Advisory Council on Maritime Cybersecurity

At IMO / regional maritime bodies: Establish a formal youth advisory panel to review drafts of cyber guidelines, risk assessments, and capacity-building proposals and voice out opinions.
Mandated consultative roll: Ensure that in all major maritime cybersecurity working groups or committees, at least one youth representative participates and contributes.
Annual youth-led review: Release an annual youth led “maritime cyber outlook” report with insights, priorities, and recommendations.

4.4 Promote Public Private Academic Innovation Labs

Maritime cyber labs: Located at ports, universities, or tech hubs, these labs bring together youth, students, port operators, and cybersecurity firms to co-create tools like intrusion detection, spoofing detection, simulation platforms.

Challenge grants / hackathons: Governments or port authorities can launch challenge based funding calls that encourage youth teams to prototype solutions, with seed funding or procurement pathways for viable tools.

4.5 Guarantee Equitable Access, Capacity Support, and Inclusion

Targeted funding: Create dedicated funds like grants, scholarships to support youth from low and middle income countries, women in cybersecurity, and underrepresented regions.
Connectivity & infrastructure support: Invest in backbone digital infrastructure (broadband, labs) for underserved maritime universities and coastal regions to enable participation.
Language, mentorship, and outreach: Translate training content into multiple languages, and pair young professionals with mentors from international networks to reduce isolation or barriers.
Monitoring & evaluation: Track youth participation (number of trainees, regional representation, career outcomes) and adjust programs based on feedback.

5. Conclusion

The accelerating digitization of global shipping systems has made maritime cybersecurity vital to economic stability, supply chain resilience, environmental protection, as well as national security. While regulatory frameworks like IMO’s MSC.428(98) mark progress, the effectiveness of cyber risk management ultimately depends on the skills, expertise, and innovative contributions of people.

Youth represent a key asset of talent, creativity, and energy. But unless institutions intentionally give importance to bring awareness through education, institutional slots, mentorship, funding, and consultation that reservoir remains underutilized. By implementing the recommendations policymakers and maritime stakeholders can bring about a sustainable, inclusive, and dynamic maritime cybersecurity system.

References:

1. https://www.darktrace.com/cyber-ai-glossary/cybersecurity-in-maritime
2. https://www.mdpi.com/2077-1312/9/12/1323
3. https://www.cyberdefensemagazine.com/global-shipping/
4. https://www.mdpi.com/2077-1312/12/10/1844
5.https://www.google.com/amp/s/cyble.com/blog/cyberattacks-targets-maritime-industry/
6.https://arxiv.org/abs/2506.15842#:~:text=A%20Sea%20of%20Cyber%20Threats%3A%20Maritime%20Cybersecurity%20from%20the%20Perspective%20of%20Mariners,-Anna%20Raymaker%2C%20Akshaya&text=Maritime%20systems%2C%20including%20ships%20and,goods%20and%20supporting%20internet%20connectivity.
7.https://www.atlanticcouncil.org/in-depth-research-reports/report/cooperation-on-maritime-cybersecurity-recommendations/
8. https://www.plymouth.ac.uk/research/cyber-ship-lab
9.https://www.mpa.gov.sg/media-centre/details/collective-efforts-to-strengthen-maritime-cybersecurity
10.https://greenvoyage2050.imo.org/kenyas-youth-positioned-to-lead-maritime-decarbonization/