IHCL LAUNCHES COMPREHENSIVE PORT SECURITY TRAINING PROGRAMS IN RESPONSE TO GROWING HYBRID THREAT LANDSCAPE

Advisory Board Chairman and Former Commander-in-Chief of Ukraine's armed forces calls new courses 'critical infrastructure for a new era of conflict'

LONDON, MIDDLESEX, UNITED KINGDOM, May 12, 2026 /EINPresswire.com/ -- The International Humanitarian College of London (IHCL) today announces the launch of the PORTS Training & Readiness Framework, a structured, multi-level security training programme designed to transform port security across the United Kingdom from compliance-based practice into genuine operational readiness.

> We have witnessed, at devastating cost, what happens when adversaries target the arteries of supply and logistics. Ports are not merely commercial assets, they are strategic infrastructure."
>
> *General Dr. Valerii Zaluzhnyi*

The programs address cyber, physical, and multi-domain threat environments, and is being launched in direct response to the rapidly evolving hybrid threat landscape facing British and European port infrastructure.

The launch has the full backing of General Dr Valerii Zaluzhnyi, Chairman of IHCL's Advisory Board, Ambassador Extraordinary and Plenipotentiary of Ukraine to the United Kingdom and Northern Ireland, and former Commander-in-Chief of the Armed Forces of Ukraine. General Zaluzhnyi, who brings unparalleled frontline experience of how adversaries target critical infrastructure as a deliberate instrument of warfare, has issued a clear message to UK port operators, security personnel, and government authorities: this training is not optional it is a strategic necessity.

"We have witnessed, at devastating cost, what happens when adversaries target the arteries of supply and logistics. Ports are not merely commercial assets, they are strategic infrastructure. A cyber-attack or physical assault on a major European port could paralyse military resupply, humanitarian aid, and civilian economies simultaneously. This is not a hypothetical risk. It is a doctrine already being employed against us in Ukraine."
— General Dr. Valerii Zaluzhnyi, Chairman, IHCL Advisory Board

General Zaluzhnyi has identified two categories of risk that make dedicated port security training an urgent priority for the United Kingdom.

IHCL colleagues with the Ambassador who is also Chairman of the IHCL's Advisory Board

Cyber Threats

Modern ports rely on deeply integrated digital systems, from automated cargo handling and vessel tracking to customs processing and energy management. A coordinated cyberattack on port management systems could halt operations entirely, disrupt the flow of military materiel and humanitarian supplies, and create cascading failures across interconnected national infrastructure. IHCL's new PORTS programme addresses this threat directly, equipping IT, OT, and cybersecurity teams with the knowledge to harden port systems, identify vulnerabilities, and respond effectively when attacks occur.

Physical Attacks

Ukraine's experience has demonstrated the capacity of state-sponsored actors to conduct precision strikes on port facilities, fuel depots, and logistics hubs. European and UK ports remain potential targets in any sustained hybrid conflict scenario.

The PORTS programme trains security personnel, operations teams, and executive leadership in physical hardening, threat recognition, access control, and integrated civil-military coordination, the building blocks of genuine resilience. It is structured across three levels, ensuring that every member of port staff, from frontline contractors to board-level executives, receives training appropriate to their role and responsibilities.

Level 1: Awareness Courses

Designed for all port personnel, these short online courses lay the foundation:

- PORTS Security Awareness Fundamentals (2–3 hours, online) — covers the modern threat landscape, hybrid threats, why ISPS compliance alone is insufficient, and basic incident reporting responsibilities.
- Maritime Threat Recognition for Ports (3–4 hours, online) — enables operations staff and security personnel to identify abnormal behaviour, suspicious patterns, and take appropriate initial action.
- Cyber Awareness for Port Personnel (2 hours, online) — reduces cyber risk exposure across all staff by addressing phishing, social engineering, cyber hygiene, and the human factor in cyber incidents.

Level 2: Operational Readiness Courses

Role-based blended learning for management, security leads, and operational teams:
- PORTS Executive Security Leadership — equips executives, port authorities, and senior management with strategic decision-making skills under modern threat conditions, including crisis governance, risk and liability, and business continuity.
- PORTS Integrated Security Management — bridges ISPS compliance with real operational security for PFSOs, CSOs, and security managers, covering integrated security architecture, incident command structures, and SOP design.
- PORTS Operational Readiness for Port Teams — develops situational awareness, escalation protocols, communication, and cross-team coordination for supervisors, control room staff, and marine operations.
- Cyber & OT Resilience for Ports — a 3–5 day modular programme strengthening the cyber-physical resilience of port systems, covering vulnerabilities in PCS/TOS/PMS environments, access control, and incident response.

Level 3: Advanced & Specialist Courses

Immersive simulation and advanced integrated training for security, operations, and command teams:
- PORTS Operations Centre Training — simulator-based training for integrated security system operators covering threat detection, sensor integration, and incident logging.
- Simulation & Scenario-Based Training — realistic multi-domain exercises training decision-making under pressure, unit coordination, and real-time response.
- Digital Twin & Red Team Exercises — advanced simulation to identify port-specific vulnerabilities, stress-test systems, and build resilience through red teaming.
- Cyber-Physical Integrated Incident Response — synchronises cyber and operational response teams through tabletop and simulation exercises covering hybrid attack scenarios and recovery coordination.
- Train-the-Trainer Programme — enables port organisations to sustain training capability internally, covering delivery methods, scenario design, and continuous readiness programme development.

Recognising that port staff cannot always leave operational environments for training, IHCL has designed the PORTS programme for maximum flexibility. Courses are delivered online, in blended formats, and through mandatory offline simulation and live exercises, allowing organisations to train staff at site or remotely according to their operational requirements.

Participants achieve certification across four levels: Foundation, Operational, Advanced, and Instructor, providing a clear, measurable pathway from basic awareness to the ability to deliver training programmes internally.

Training is structured across an annual cycle: Assessment & Awareness; Role-based Training;

Simulation & Exercises; and Integrated Drill & Certification — ensuring readiness is maintained, not just achieved.

General Zaluzhnyi has been unequivocal about the urgency facing the sector. His message to port operators and the authorities responsible for UK maritime security is direct:

"Every week of inaction is a week that our adversaries use to probe, plan, and position. Europe's ports are a gift to those who wish to destabilise our societies and sever our alliances. We must not offer that gift freely."— General Dr. Valerii Zaluzhnyi, Chairman, IHCL Advisory Board

IHCL is partnering with key industry suppliers and port authorities to make the PORTS programme available to port staff and organisations across the United Kingdom. The College urges port operators, security managers, and government bodies to engage with this programme as a matter of priority.

Dr. Serhii Kosianenko
International Humanitarian College London
+44 20 3807 4597
email us here
Visit us on social media:
LinkedIn
