

Project Title: “Cybersecurity: Risk Management from Advanced Technology to Law and Insurance for Maritime and Aviation Logistics Operations”

研究項目: “數位科技安全：從先進科技到法律及保險的風險管理應用於海事和航空物流行業發展”

Investigator: Dr WONG Eugene Yin-cheung (PI), Dr Linsey CHEN (Co-PI)

Funding Scheme: Research Grants Council - Inter-Institutional Development Scheme (IDS)

Project Reference No.: UGC/IDS14/B03/19

Abstract

With the increased use of digital platforms, the Internet of Things (IoT), automation and cyber-physical systems in maritime, aviation and logistics operations, the threat of cyber-attacks has become one of the topmost concerns in this sector which involves highly connected systems and networks along the whole supply chain. Individual threats include viruses spreading through networked systems, cyber-attacks on operations platforms and the hijacking of sensitive data. Any one of these attacks would seriously impact daily operations and incur huge losses in operational costs, such as through stoppages of cargo movement, misrouting, vessel or flight delay, data leakage, system breakdowns or power outages. The recent cases of Maersk and Cathay Pacific highlight how disruptive and expensive such threats can be.

Governments are struggling to determine proper measures for dealing with the ever-increasing receipt of daily threat alerts and data breaches from advanced malware, zero-day exploits and persistent threats. International professional associations such as the International Maritime Organisation (IMO) and the International Air Transport Association (IATA), have sought to develop guidelines, rules and regulations for cybersecurity and risk management. In Hong Kong, whose port container throughput has been ranked in the top ten for decades and air cargo first since 2010, the government’s ability to maintain its competitive position depends on security measures to ensure smooth logistics and transportation operations. Promoting and supporting Hong Kong as an international maritime logistics hub providing high value-added maritime services has been one of the key items in the government policies. These include peripheral and high value-added services such as maritime law and arbitration, aviation and safety regulations and maritime insurance. With operations and communications in global maritime, aviation and logistics sectors now highly reliant on digital technology and Internet support, risk management strategies and legal knowledge are crucial for ensuring that daily operations remain cost-effective and smooth. Lacking research, education and technology for improving cybersecurity in maritime and aviation operations as well as significant gaps in international regulations are found, leading to insufficient knowledge and experience of industry practitioners in tackling this increasingly complex problem.

This project will organise a research workshop and international forum tailored for logistics practitioners to discuss cybersecurity and risk management for maritime and aviation logistics, from advanced technology to legal and insurance perspectives. At these events, participants will evaluate both overseas and Hong Kong case studies, which will be compiled and shared on an online learning platform and in a reference book. The participants will also discuss Hong Kong and China’s cybersecurity development strategies for maritime Silk Road ports. Together, the platform and reference book will provide detailed insights for maritime and aviation cybersecurity, tailored to students and practitioners using the up-to-date cases from Hong Kong, China and the broader region.

