Dr Spyros Papastergiou,
University of Piraeus Research Center, Greece

Short Curriculum Vitae (C.V.)

Dr. Spyridon Papastergiou has received B.Sc. in Computer Science, M.S. degrees in Advanced Information Systems (Network Information Systems) and Ph.D. in Security, Privacy and Interoperability of m/e-services from the University of Piraeus, Greece in 2004, 2005 and 2009 respectively. Since October 2005, he is security researcher in the University of Piraeus Research Centre and member of the Information Security Laboratory at the Informatics Dept. of the University of Piraeus. His research interests lie in the areas of security, privacy and interoperability of mobile/electronic services, strategies for the anonymization of e/m transactions as well as assessment and management of risks and threats associated with Critical Infrastructures; he has authored over 20 publications in these fields. He has been involved in a set of European (e.g. SELIS/eTen, SWEB/IST, ImmigrationPolicy2.0, CYSM, DAEDALUS, Medusa, MITIGATE and OPERANDO) and national research projects (e.g. PENED2003 and S-PORT) and has active participation in six Cyber Defence Exercises organized by the Hellenic National Defence General Staff (1st, 2nd, 3rd and 4th National Cyber Defence Exercises ("PANOPTIS 2010", "PANOPTIS 2011", "PANOPTIS 2013" and "PANOPTIS 2014"), ENISA (European cyber defence exercises (CyberEurope 2014)) and NATO (NATO «CYBER DEFENCE EXERCISE 2010 (NCDEX 10)). In addition, he has worked for more than 6 years as Security Consultant specializing in Information Security Technology Implementation and Integration and Risk and Vulnerability Assessment.

"Assessing the Risk of Ports Supply Chains and Their Cascading Effects"

In the modern era, maritime transport chain is a complex network where various organizations interact with each other in order to support and provide a number of Supply Chain Services (SCS). These services have significant impact on the local, regional and European business and manufacturing sector since they ensure the effective and efficient transport of people, freight, natural gas, oil, cargoes and manufactured goods. Usually, the SCS involve various operations including physical operations (stevedoring, loading, unloading, storage, transportation, inspection, etc) as well as information and data flow operations through networks, document management systems, databases, portals, etc (forwarding, invoicing, pre-arrival notifications, customs clearance documentation management, ISPS declaration, etc) between the maritime authorities or/and the contracting entities involved in them in any way.

However, several recent studies have shown that the threats landscape is changing continuously; thus, the malicious users will continue to do the unexpected discovering new ways to break into processes and operations of the maritime supply chain. To this end, significant research efforts have been made towards risk assessment methodologies especially suited to Critical Infrastructures (CIs). In principle, most of the risk assessment methodologies focus on the identification of threats, vulnerabilities and the related impact and ultimately on the evaluation of the underlying risks failing to address the cascading effects occurring from cross-sectoral and/or cross-border dependencies. As a consequence, they tend to focus on organization-wide risks and they fail to capture the security needs of more complex eco-systems of interdependent organizations. The main goal of this presentation is to illustrate the work undertaken in the MEDUSA project in order to alleviate the above-mentioned gap, through introducing, specifying and validating multi-dependency approaches to risk assessment.