INTERNATIONAL CENTRE FOR CHEMICAL SAFETY AND SECURITY (ICCSS)

OPCW Roadmap to improve chemical industry resilience to cyberattacks

ICCSS offer for international stakeholders

CONTACT: **Mr. Adam Paturej;** Director Cybersecurity and Reliability Program ICCSS
ul. Leszno 8/1; 01-192 Warsaw; Tel: +48 22 436 20 44: www.iccss.eu

OPCW Roadmap to improve resilience to cyberattacks

2013 and 2015 UN Group of Government Experts (GGE) reports identified a four-pronged approach to global cyber stability:

1. Develop acceptable norms of state behavior, and clarify how exactly international law applies;
2. Enhance transparency, co-operation, and stability between States in cyberspace through confidence-building measures;
3. Enhance international co-operation;
4. Build national/international capacities to deal with cyber challenges.

Most of international organisations have not developed measures to protect their activities and national and local partners from cyberattacks. It is a result of a legal situation since internal security, which includes cybersecurity, remain within national competences.

The international organisations, especially in the domain of industry, health, environmental, chemical, bio, nuclear, areas should assume a leadership role to advance cyber security of their related activities and plants, including their computer networks and Industry Control Systems (ICS), in cooperation with the international partners.

Support to an increase of resilience and cybersecurity of chemical installations should be an element of the international organisations wide strategy to reduce cyber threats and enhance safety and security.

The international organisations active approach towards cybersecurity should include promotion of knowledge and the adequate security systems against cyberattacks among all the stakeholders in their related industries, including critical infrastructure, especially in the developing countries.

The chemical community should participate in the dialogue on the subject of the existing resources and requirements which should be met in order to counteract potential cyberthreats and minimize potential losses.

The international organisations should assist in raising awareness of threats coming from cyberattacks, and the implementation of effective technical solutions. Such an collective engagement could constitute a specific kind of international organisations roadmap.

The leading assumption of the international organisation roadmap will be a statement that the traditional crisis responses are insufficient to battle the challenges resulting from accidents and catastrophes caused by cyberattacks. In order to battle the potential cyberthreats, we need the co-operation between all entities (community commitment).

The initiative of a international organisation roadmap for raising cybersecurity awareness and sharing best practices among users of the relevant industries should be a part of the broader efforts to enhance chemical safety and security.

The core objective of the international organisations roadmap would be the creation of a cybersecurity culture and practices among the relevant activities and stakeholders. State agencies, producers and users of the chemical industry including industry associations, economic chambers and social organisations should be partners of the international organisations roadmap. The roadmap would include the development of international organisations led information exchange about cyber threats in their activities.

Within the international organisations roadmap, an international organisation Working Group should function to support its implementation, with the participation of government, private sector, industry, civil society and media.

The Working Group should offer a platform for co-operation among all the stakeholders. It should develop a system of information exchange about cyber threats and the promotion of a cybersecurity culture. Within the Working Group best practices, standards, national and industry capacity building measures, training solutions and exercises, should be developed and shared.

INTERNATIONAL ORGANISATIONS CYBERSECURITY SYMPOSIUM	
Objectives:	To build awareness of the (increasing) threat and risks emanating from cyber-attacks on chemical facilities. To explore possibilities to create a comprehensive framework for enhancing information networks' security, and to improve the preparedness for, prevention of, and response to cyber-attacks; To develop the international organisation Roadmap for cybersecurity awareness and sharing best practices.
Description of Activities: Specific actions or processes undertaken to convert the project into the outputs, including assessment of existing standards and best practices in place.	• A1 – Awareness build-up of the threat among stakeholders/participants • A2 – Discuss the need to effectively gather information about cyber threats (including, for instance, intentions to use the information network as an improvised Chemical device) • A3 – Discuss the need to create an effective administrative and/or regulatory framework to address cyber-attacks • A4 – Make an inventory of experience and expertise available in order to create a working group o explore the possibilities of an integrated, inter-agency approach to address the threat of cyber-attacks • A5 – Discuss and demonstrate advantages of multi-stakeholder approach • A6 – Render support for the assessment of current practices as well as the development/identification of methodologies and tools for situation and needs assessment, and effective awareness raising measures to be implemented with the involvement of stakeholders
Deliverables: An output produced by the activities of the work package, for example, guidelines for industry experts on cybersecurity	• D1 – Working paper with an outline of the objectives, activities, and outcomes of the Symposium • D2 – Comprehensive assessment of the threat, existing capabilities, vulnerabilities and shortfalls • D3 – Guidelines to ensure minimum level of preparedness to cyber-attacks • D4 – Creation of a working group, based on, for instance, an inventory of existing and required resources (personnel, equipment, other material)
Milestones: Control points where decisions are needed with regard to the next stage of the project.	• M1 – Evaluation of safeguards against cyber-attacks currently in place • M2 – Evaluation of steps taken for creating a working group • M3 – Initiatives taken to realize follow-up (events) • M4 – Identify opportunities and requirements for follow-up measures to further the process of enhancing cyber-security
Expected Results: Changes or effects that the project expects to bring about, including the OPCW measures to support cyber-security in chemical plants	• R1 – Increased awareness of the dangers of cyber-attacks on information systems of chemical facilities • R2 – Enhanced efforts to address cyber-attacks, coordinated/led by working group

INTERNATIONAL CENTRE FOR CHEMICAL SAFETY AND SECURITY

Working together to enhance chemical safety and security

ul. Leszno 8/1
01-192 Warszawa
Polska
(phone – office) +48 22 436 20 44

www.iccss.eu ; info@iccss.eu