Critical Infrastructure Protection & Resilience

European Reference Network for Critical Infrastructure Protection

Our mission is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities.

erncip

newsletter no. 19

2nd IMPROVER-ERNCIP Joint Operators Workshop 2017

Critical Infrastructure Resilience

May 11-12 2017, Ispra

- Day 1: Improving organisational resilience for critical infrastructure operators
- Day 2: Achieving community resilience in collaboration with critical infrastructure operators

Researchers, operators and the IMPROVER consortium joined forces for two days of presentations, knowledge sharing, and networking. This joint operators' workshop brought together the communities of ERNCIP and the IMPROVER project.

Previous events had focused on the technical aspects of resilience, while this year's themes were organisational and community resilience. The workshop was also an opportunity for the IMPROVER project consortium to present its activities and results in order to get feedback from critical infrastructures operators.

Check out a video of some of the feedback we received: https://vimeo.com/220636901/7dc07c7afe. The presentations of the workshop are available on the ERNCIP website: https://erncip-project.jrc.ec.europa.eu/events/2nd-improver-erncip-joint-operators-workshop-2017

IACS Thematic Group

TG EU IACS Components Cyber-Security Compliance & Certification Scheme

Publication of Proposals for IACS Cybersecurity Certification Framework

The report "Introduction to the European IACS components Cybersecurity Certification Framework (ICCF)" was published in mid-March 2017 and is available for download at: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf. It proposes an initial set of common European requirements and broad guidelines to help foster IACS cybersecurity certification in Europe, describing the Framework with recommendations for governance, adoption and implementation.

ICCF kick-off meeting 23 May Paris

The ERNCIP Thematic Group on ICCF resumed its work on a European IACS components Cybersecurity Certification Framework with this kick-off meeting to agree the work programme for 2017/2018. The main goal is to "challenge" the ICCF through exercises that will simulate "the behaviouristic and governance model" of the Framework, in cooperation with stakeholders operating in "National Exercise Groups" (NEGs). The experts agreed to provide the results of the NEGs by November 2017 so that the feedback can be used to finalise the ICCF feasibility study, for release in March 2018.

The Group will explore constraints, limits, success factors and enablers that can influence the implementation of a European certification framework in the future, and will contribute to the definition of the Roadmap for a European ICT security certification framework for product and services, foreseen by the end of 2017.

ERNCIPnewsletter
Technology Innovation in Security
Space, Security & Migration, European Commission
21027 Ispra (VA) Italy
https://erncip-project.jrc.ec.europa.eu/

Contact Georgios Giannopoulos
European Commission, Joint Research Centre
Space, Security & Migration - Technology Innovation in Security
Via E. Fermi 2749, I-21027 Ispra, Italy
e-mail: jrc-erncip-office@ec.europa.eu
Tel +39 0332 786045 - Fax +39 0332 786565

Radiological and Nuclear Threats to Critical Infrastructure Thematic Group

Joint JRC/GICNT workshop

On 28-30 of March, 2017, the European Commission's Joint Research Centre (JRC) and Nuclear Detection working group of the GICNT (Global Initiative for Combatting Nuclear Terrorism) co-organised the Magic Maggiore: Technical Reachback Workshop. This proved to be a great success involving around 70 technical, scientific, and policy experts from 25 countries of which 13 were non-EU including the USA, Russia, China and Japan. This wide participation is a clear indication of the importance of international activities for global security against nuclear terrorism.

The Workshop facilitated discussion among experts from the nuclear security field regarding the roles and responsibilities, challenges, and opportunities for technical expert support within existing Nuclear Security Detection Architectures.

Also, a multi-site demonstration was arranged of how national and international reachback might work in practice. The JRC and the French Alternative Energies and Atomic Energy Commission (CEA) successfully linked a simulated nuclear border incident to the CEA centre in Paris, with two-way transfer of radiation detection information, while displaying the events playing out at both locations to the workshop participants through live streaming. This demonstration exemplified the theoretical/conceptual discussions of the workshop, and highlighted the importance of interoperability of technical solutions and procedures towards the objective of improved security against RN threats.

Innovative detection technologies, use of robotics, and technical reach back

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to identify how nuclear security can benefit from emerging technologies, such as new materials and segmented detectors, and to identify how they can utilise the new list-mode data acquisition standard. The Group will also define the characteristics of a centralised data management system that will efficiently support assessment and adjudication of nuclear alarms and alerts.

ERNCIP Externally

Hybrid Threats

Developing tools and vulnerability indicators for hybrid threats in critical infrastructures

Workshop: 4-5 of May 2017, Brussels

The JRC, in collaboration with DG HOME, organised this workshop on Hybrid Threats, with the participation of 24 Member States, NATO, the INTCEN Hybrid Fusion Cell and the point of contact for the newly established Centre of Excellence for Hybrid Threats in Finland. During the preparatory phase of this workshop, the JRC issued a questionnaire to Member States addressing the main topics in the domain of Hybrid Threats.

Key points to come out of this meeting were:

- The main issue in hybrid threats is to detect that a hybrid threat is really taking place before it escalates to a crisis. Once it becomes a crisis there are mechanisms at national and EU levels in order to respond
- Detecting an ongoing hybrid threat requires the correlation of several streams of information. This is a challenge considering the confidential nature of such information and the restrictions in sharing this among stakeholders
- A one-size-fits-all composite indicator should be avoided. Instead there is a need for several indicators that provide a comprehensive overview of whether a hybrid threat is under development.
- It is important to connect detection indicators with vulnerability indicators
- Operators expressed the need for better information sharing mainly because in the domain of hybrid threats the problem is very complex and by definition operators can only see bits and pieces of the puzzle which prohibits them to understand whether a hybrid threat is under development
- The components presented by the JRC namely technological, media, societal cover sufficiently the topic. These components constitute the attack surfaces, with the technological component (critical infrastructures) being an extremely important aspect and a very important entry point for Hybrid Threats. In the view of most Member States, Hybrid Threats aim at reducing the capacity of a country for decision making.

The JRC is now drafting a report on the basis of the questionnaire and the outcomes of the workshop, to be shared with the Member States for comments and suggestions. This report will also describe the next steps in terms of tools and vulnerabilities indicators development. By the end of 2017 a second workshop will take place in order to validate the work that will be conducted by the JRC during 2017.

Number 19
January - May 2017
JRC107401

Thematic Groups in Summary

Detection of Indoor Airborne Chemical-Biological Agents

Protecting against airborne CB threats

During the its initial year of work, this Group has identified major issues to be addressed in the EU level regarding Detection, Identification and Monitoring (DIM) of airborne, chemical and biological threats in enclosed spaces, based on reviews of chemical and biological sensors, and of numerical simulation. The Group has been commissioned for two more years by DG-HOME to assist security managers in implementing a comprehensive plan for protection against such threats, through the application of a combination of available technologies.

The Group will now investigate sensor systems, including interoperability requirements of components, and the optimal combination of technologies for early and effective detection and identification, expanding its research to issues such as the use of omics techniques for the post-event identification/verification of threats. The main output of the group will be guidance to security managers on the optimal setup of sensor systems against airborne threats.

Chemical-Biological Risks to Drinking Water

Guidance for production of water security plans

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to produce a European-level guidance document that will support water utility operators to produce a water security plan, devoted to improving water security.

In particular, the group will identify the current approaches to screening for contamination using online monitoring and event detection systems, investigating in particular issues to operators arising from the reliability of the detection methods and taking into account additional analytical procedures.

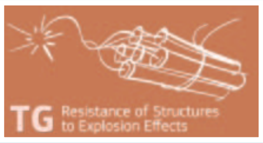
Detection of Explosives and Weapons in Secure Locations

Vehicle Screening for Weapons and explosives - CEN workshop agreement

This Group has been commissioned by DG HOME (Innovation and Industry for Security) to undertake the activities necessary to create the relevant standardisation mechanism, probably a CEN workshop agreement (CWA), for production of European-level guidelines for security managers regarding the screening of vehicles at entry checkpoints, for weapons and explosives, by 2019.

Protection of Structures and Soft Targets

Risk-based approach for securing buildings against terrorist attacks



This Group has been commissioned by DG HOME (Innovation and Industry for Security) to study possibilities to introduce a risk based approach for the security of buildings under terrorist attacks in the building standards (EUROCODES) or similar other standards. In addition, CEN TC 33 will be supported concerning the revision of the standards for testing building products under blast loading.

Extended Virtual Fencing

Use of biometric and video technologies

The ERNCIP Office is currently establishing a new Thematic Group on “Extended Virtual Fencing - use of biometric and video technolowgies” to run for two years with an initial aim to produce a “state of the art” report by the end of 2017. This will assess the current opportunities afforded by these technologies for more integrated solutions to provide improved protective security, e.g. by virtually extending boundaries. In order to achieve this, ERNCIP is seeking European experts to become involved in the Thematic Group. Expressions of interest can be sent to: JRC-ERNCIP-OFFICE@ec.europa.eu

Future ERNCIP meetings

ERNCIP Group of EU CIP Experts
12 July 2017, Ispra

Meeting of the ERNCIP advisory body formed of experts nominated by the Member State authority responsible for critical infrastructure protection.

TG Detection of Indoor Airborne Chemical-Biological Agents
5 Sep 2017, Ispra

Kick off Meeting of the group to start working on creating a guidance for security managers.

TG IACS Cybersecurity Certification Framework
22 Sep 2017, Brussels

Meeting of National Exercise Groups to review progress of their challenges to the proposed Framework.