Second ERNCIP Operators Workshop

Workshop report

Klaus Keus
Carmine Rizzo
Alois J. Sieber

2014

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Report EUR 26858 EN

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Naouma Kourti
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 721, 21027 Ispra (VA), Italy
E-mail: ern-cip@jrc.ec.europa.eu
Tel.: +39 0332 78 6045
Fax: +39 0332 78 5469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC91831

EUR 26858 EN

ISBN 978-92-79-42602-5

ISSN 1831-9424

doi:10.2788/17555

Luxembourg: Publications Office of the European Union, 2014

Printed in Italy

European Commission

Joint Research Centre

Second ERNCIP Operators Workshop

JRC, Ispra (Varese),
Italy
19 and 20 May 2014

Workshop report

Authors:
Klaus Keus
Carmine Rizzo
Alois J. Sieber

Joint Research Centre

The European Reference Network for Critical Infrastructure Protection (ERNCIP)

Contents

1. Executive summary

The participants at the Second Operator's Workshop welcomed the meeting, underlining their appreciation that ERNCIP is listening to the problems and needs of operators of critical infrastructures (CIs), and invited ERNCIP to consider organising such events more often. The operators underlined that they need a political action to encourage input from research and innovation, as well as for operational matters. Harmonised EU procedures and harmonised legislation are necessary to improve coordination at the European and global levels, and to ensure a common level of security-related requirements and a fair financial burden for the operators' business. A major challenge consists in measuring and estimating risks, as well as calculating or estimating costs. Scenario-oriented approaches — related, but not limited, to risk assessment — would enable a more structured process, as would new models for risk and costs estimation. Financing and related investments are challenges that have a direct impact on business, and hence on competiveness.

Reviewing ERNCIP's present efforts, the existing thematic areas seem to be scattered from an operator's point of view, and an umbrella structure reflecting the sectorial relevance is missing.

Moreover, the operators underline the need to link security with existing safety efforts. One example is '**safeurity**' — a concept being developed within the rail sector addressing the interdependencies between safety and security. The main aim is to clarify and provide a structured method to establish comprehensive protection of infrastructures and operations — of any kind.

The participants pointed out that no EU-wide harmonised training for operators exists, and neither does the certification of qualified personnel. They asked ERNCIP to facilitate the creation of such a training scheme. The repository of threats and vulnerabilities of CIs that has been requested previously should be used as a basis.

Moreover, operators feel that insufficient information is available about security research efforts at the EU, as well as at the national, level. At best, only promotional types of leaflets are available, such as through the EU's CORDIS[1] website. It is highly desirable that operators can get an overview of what research has been sponsored so far in the context of critical infrastructure protection (CIP) at both EU and national levels. In particular, operators want to be informed about research results, the impact of these projects and how the results achieved will be exploited to increase the security of CIs.

Participants invited ERNCIP to facilitate the production of this information as well as a dialogue between the managers of the research programmes and CI operators. By doing so, gaps and needs for further research can be established and the innovation process, the core of Horizon 2020, the EU framework programme for Research and Innovation, can be promoted.

2. Background information

The Institute for the Protection and Security of the Citizen (IPSC) of the European Commission's Joint Research Centre (JRC) set up the ERNCIP project in 2009 under the mandate of the Directorate-General for Home Affairs, in the context of the European

[1] http://cordis.europa.eu/

programme for critical infrastructure protection (EPCIP) and with the agreement of Member States. The preparatory phase was successfully completed in November 2010 and the implementation phase started in 2011.

ERNCIP aims to provide a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of CI against all types of threats and hazards.

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

It is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier to future development and market acceptance of security solutions.

ERNCIP addresses several thematic areas (TAs), as identified by its sponsors, i.e. the European Commission and the Member States. The work is being undertaken by specific thematic working groups, each led by a coordinator. A work programme is established by each thematic group (TG) and approved by the ERNCIP office.

Currently (June 2014), ERNCIP covers eight thematic areas:

- aviation security detection equipment;
- explosives detection equipment (non-aviation);
- industrial automation and control systems;

- the resistance of structures to the effects of explosions;
- chemical and biological risks in the water sector;
- video analytics and surveillance;
- applied biometrics for CIP;
- radiological and nuclear threats to critical infrastructure.

More information about ERNCIP, including projects, an inventory of CIP experimental capabilities, thematic areas, newsletters and many other documents, is available at:

https://erncip-project.jrc.ec.europa.eu

3. Introduction and workshop objectives

The Second ERNCIP Operators' Workshop took place in Ispra (Varese), Italy, on 19 and 20 May 2014, at the JRC premises. The workshop consisted of three sessions, attended by 31 high-level professionals representing operators' organisations from all over the European Union. Also taking part were three moderators (one for each session) and several representatives of the ERNCIP staff of the JRC, who coordinated and supervised the preparation and conduct of the workshop. The operators taking part represented the energy, information and communication technology (ICT), transport, water and consultancy sectors, as well as wider industry.

The objectives arose from the First ERNCIP Operators' Workshop, which took place in Brussels on 12 and 13 September 2013. This first workshop highlighted major operators' needs in terms of risk management, crisis management and technology. Lessons learnt related to the relationship between generic needs and sector-specific needs, and above all a strong need for more exchange among operators and sectors. For more information see:

https://erncip-project.jrc.ec.europa.eu/networks/opworkshops

As a result, the overall objective of the Second ERNCIP Operators' Workshop was to cater for the need for more exchange among operators and sectors, and to identify how to develop and leverage ERNCIP's role for the benefit of the operators of CIs. The workshop was therefore structured in three closely linked sessions, during which the operators participated actively in the flow of discussions, from the operators' challenges related to the assessment, selection and

deployment of technological security solutions (Session 1) and tools and instruments to address such challenges (Session 2) to, based on the outcome of these two sessions, how ERNCIP can develop its role on an EU level to best help operators (Session 3). Each session was centred around a driving question.

- Session 1, moderator Mr Klaus Keus: *What are today's challenges for operators regarding assessment, selection and deployment of technological security solutions?*
- Session 2, moderator Mr Carmine Rizzo: *What tools are available for operators and how can these be best utilised in order to address the above challenges regarding the assessment, selection and deployment of technological security solutions?*
- Session 3, moderator Mr Alois Sieber: *How can the ERNCIP network help to address these challenges on an EU level?*

In Sessions 1 and 2, the operators divided into three working groups representing the following CI sectors: energy, ICT and transport (the operators from the water sector joined those from the energy sector). After the discussions, a rapporteur for each sector provided a briefing to all participants, moderators and ERNCIP staff. For these two sessions, this report provides the outcome from the discussions for each sector, and an overall analysis. Special thanks go to the rapporteurs: Ingo Jensen and Robert Rodger for energy, Gerald McQuaid for ICT and José Pires for transport.

Session 3 comprised an open discussion among all participants developed out of Sessions 1 and 2. In addition, 'green cards' were distributed to all participants on which they could openly express any other thoughts, and these were reviewed and taken into account after the

workshop. For this final session, this report provides the overall conclusions of the workshop, including some remarks and recommendations.

4. Report on Session 1 (Operator challenges)

Driving Question for Session 1: What are today's challenges for operators regarding assessment, selection and deployment of technological security solutions?

The addressee of this question is the operator and the core focus is on challenges related to technological security solutions, and specifically the phases of assessment, selection and deployment of such solutions, through a process illustrated in Figures 1 (funnel view) and 2 (cyclical view) below.

To offer some initial guidance as an input for discussion, in the preparation phase of the workshop, the ERNCIP team predefined several topics to cover the main areas of the broad range of possible issues, including, but not limited to, risk awareness, the legislative framework, assessment/testing, guidance and financing.

Although the three selected sectors (energy, ICT and transport) are not fully inclusive of all current active thematic areas within ERNCIP, the outcome of the workshop discussion provided orientation and guidance for an overall ERNCIP approach.

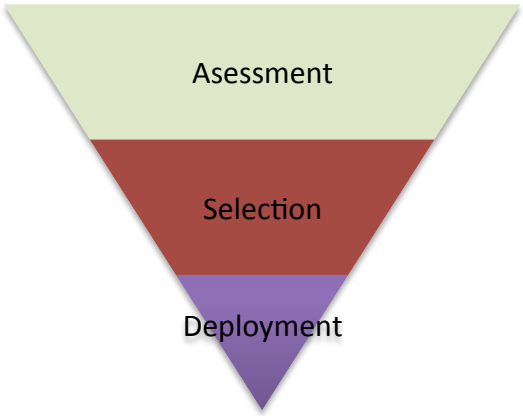

Figure 1: Funnel view of the phases of the process of assessment, selection and deployment of security technological solutions

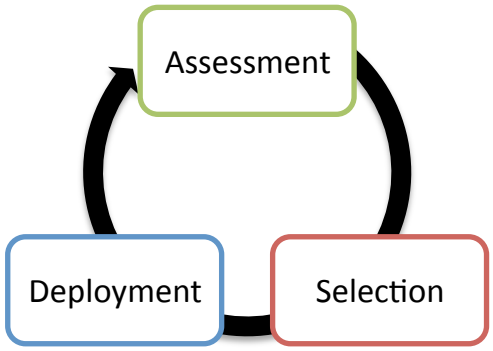

Figure 2: Cyclical view of the phases of the process of assessment, selection and deployment of security technological solutions

Energy

With regards to the increasing international orientation of the energy business and its global competition, a detailed knowledge about different sets of national legislation and regulations is a challenge for players in this market. The inadequacy or lack of harmonised European or international legislation contributes to, and increases, the uncertainty. To reduce such challenges, a first beneficial step would be to create an inventory of related legislation.

Even if many offers of certified security training for operators exist — mostly national or even (enterprise- or sector-specific) proprietary and independent solutions — the underlying requirements are not harmonised and a cross-border or mutual recognition as certified professionals is not yet established.

In the area of risk assessment, a scenario-oriented view — applicable for multiple purposes such as training, risk assessment, security testing and validation — is still not applied. Existing and successfully used safety features might be transferred or transformed to security ones, which would require a better understanding of risk assessment, in order to distinguish between safety and security risks.

The knowledge about and the understanding and use of existing insurance cost models would support a justification for security investments. But there is not much data available on insurance factors so far, or if data is available it is not well known, and its feasibility for security is not yet proven. It would be important to involve representatives from insurance companies at a future workshop. Standards offering reasonable guidance for operators need to be more tailored to the specific needs of operators in the energy sector.

In the discussion within the plenary session, the following main issues were raised. How far is it possible to perform reliable measuring and estimating of risks? Is there sufficient information and knowledge available to perform a reliable calculation of possible risk-related costs? What about the unthinkable, i.e. those events we are not able to estimate, so-called uncertainties? Events with a low probability but potentially high impact, such as extreme space weather, should also be considered. The plenary suggested taking actions supporting the sector in this challenge for commercial and business reasons.

Some challenges and recommendations are very specific to the energy sector. The necessary European and international view of the often cross-border and globally acting enterprises in the

energy market implies a whole set of challenges relating to European and international harmonisation and mutual agreement, for example in the area of legislation, for security training or for adequate international agreed standards in guidance to operators.

Information and communication technology

In the area of risk awareness, a wide range of information and related tools, and project results, are publicly available. Nevertheless there is still a lack of qualified training in relation to risk awareness in different areas. This concerns education/training in both the academic environment and in business schools. These challenges include the manager's need for better understanding of risks in order to be better prepared for decision-making. The speed of change and the related fast developments result in greater dependencies between people and processes/systems within the knowledge base.

The lack of a 'big picture' implies less focus on systematic risk assessment and more on an ad hoc approach depending on the specific experience and knowledge of the individuals.

The lack of a clear separation between security and functionality leads to, or contributes to, misunderstandings about risk awareness and related conclusions. Hence there is a strong need to improve education related to risk awareness, including a clear distinction between IT security ([2]) (i.e. confidentiality, integrity, availability (CIA)) and functionality issues (e.g. dependability). This matter is often misunderstood or underestimated by IT people, and can

([2]) The terms IT security (information technologies) and ICT security (information and communication technologies) are used interchangeably; the expression 'cybersecurity' is used mainly as a subarea of ICT security, restricted to its features in combination with networking; 'digital security' is used as a common expression representing IT/ICT security and cybersecurity.

thus lead to additional risks.

In addition, it is necessary to distinguish between safety and security, and related risks, even if the separation might become more blurred as the relationship between them becomes closer (safety-by-security). The relevance of these needs is not restricted to CIP but is valid for IT and IT security in general.

There are several challenges related to legislation. The upcoming EU directive on network and information security ([3]) addresses EU-wide harmonised and centralised information sharing between Computer Emergency Response Teams (CERTs), relevant agencies and institutions and CIP entities (industry, government and public administration, etc.). However more clarification is needed in order to define more concretely which CI sectors should be taken into account (prioritisation) and how information should be shared. Governments are requesting open data — for example, as a contribution to the economic assessment of a CI. Even if a lot of influences from globalisation are taken into account (for example, from the UN or the United States), building trust is a central challenge. Regional effects should be considered as a possible input. But it is not clear if legislation would help or hinder.

Even if risk assessment is a bottom-up approach, a complete enterprise-wide risk assessment is needed. Assessment procedures should be conducted from the single elements to an overall enterprise-wide view, covering the whole range of different kinds of risks and risk areas, and avoiding a separation between detailed risks such as technical risks and overall risks for the enterprise. It is necessary to take into account the entire lifecycle and not restrict the view to the starting point in time. If large parts of components and products are COTS (commercial off-the-shelf), qualified risk assessment may become a new challenge.

Assessment and testing of both existing and new systems is a challenge, and it becomes an

([3]) Draft version available at: http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1666

increasing practical challenge when modifications or updates take place, also with regards to the constantly changing threat environment. An additional practical challenge, which is increasing, concerns the issue of supply chain assurance, which requires a more comprehensive approach, i.e. considering all kind of different risks, from technical via legal to organisational ones. Some very specific evaluation instruments that already exist — often product- and/or functionality-oriented, and not really designed for system evaluation — such as ISO15408 (the former Common Criteria for Information Technology Security Evaluation (CC)) or SECAM (Systems Engineering Capability Assessment Model) may play a supportive role but will not suffice to cover the total range of needs.

A further challenge is dealing with the understanding and demarcation of evaluation ([4]) compared to testing (e.g. confirmation testing or compliance testing). Both instruments have to be understood. What is the value of product evaluation compared to 100 % system testing, even if 100 % testing might not be possible for very complex products and installations (e.g. the recent case of 'heartbleed' ([5]), and can a testing environment be set up for 100 % testing? The role of models of complex systems was discussed as a possible instrument to support testing of such systems (i.e. de-composing complex systems into subsystems which can be tested; by using models it is possible to aggregate test results in order to aim for test results covering the complete complex system.) Testing may be possible for a 'time-to-market' case, which is much

([4]) IT security evaluation is considered a more destructive approach in contrast to testing which is a more constructive approach

([5]) 'Heartbleed' is a security bug in the OpenSSL (secure socket layer) cryptography library, discovered and then fixed in April 2014. Among many threat scenarios, it can be considered as a worst case one, as it highlights the difference between theoretical evaluation and practical use, and potentially has a very high impact. Consequences include: large number of highly sensitive systems (web servers) affected in various application areas (public authorities, banks, e-commerce, social networks, etc.); loss of confidence in encryption tools and open source products; efforts that operators of web servers need to expend to deploy countermeasures; amount of time necessary to implement such measures; and overall loss of reputation for operators of web servers (hence loss of trust in IT security mechanisms).

more difficult for classic CC-based product evaluations. A comprehensive combined evaluation and testing approach as mentioned previously may help to build a basis for evaluation of scenarios which are still missing and/or not addressed at all. Understanding and evaluating scenarios may help towards resilience orientation as an additional complement to traditional evaluation and testing.

Guidance for operators is often not clear or easy to understand. Sometimes it may conflict with information from peer publications. The mentality of 'box ticking' is widely used; holistic risk assessment might be a better approach. Guidance is needed for different levels of hierarchy addressing different requirements from the management level down to expert level, as there is no 'one-size-fits-all' approach. Tailored guidance is required for the strategic (management) level through the tactical (middle management level) to the operational level, to address their specific needs.

Another challenge is the realistic understanding of (technology)-driven risks (see also risk awareness and related risk assessment) as a continuous challenge. As guidance is a continuous challenge, a 'set-and-forget' mentality is a dangerous approach. Financial-based decisions may become the leading approach and may result in offloading risks by taking out insurance or leading to 'out-of-the-box' solutions.

The cost of investing in security may become a matter of competiveness, since it might become a strategic factor and possibly be seen as a burden. As the benefits and the positive contribution of IT security itself are not easy to justify, the return on investment is difficult to evaluate. Hence it is the underlying legislation or regulation which has to ensure or regulate the same weighting for all. Even if investments in ICT security are justified as improving the competiveness of the enterprise in a global market, the related proof is difficult to perform and results are difficult to measure. In addition it is difficult to select the most important areas for

investments. The provision of guidance to operators to enable them to optimise their investments is a real practical challenge, as long as the assessment of risks is still another fundamental challenge.

An additional challenge is dealing with safety and quality as complementary elements to be considered and linked to security.

A concrete example was discussed in the context of the requirements with regards to the morals and ethics related to ‘industry 4.0’ (project promoting the computerization of traditional industries such as manufacturing) and related machine-to-machine (M2M) interfaces. Increasingly machines are doing tasks which humans used to do. The related moral and ethical frameworks are no longer applicable in the same way as before. So there is a need to establish and develop more appropriate controls for the M2M devices to ensure more appropriate decisions.

ICT and in particular ICT security is a two-dimensional issue. In the vertical dimension, it is a security feature expressed by functions such as confidentiality, integrity or availability. In addition, ICT and related ICT security may be understood as a horizontal topic, i.e. as ‘key enabling technology’ (KET) and related to applications featuring security objectives. In this context ICT security delivers a ‘security enforcing functionality’ to ensure, or at least to contribute to, the security functioning of the application.

There seem to be no specific issues for ICT security (features or conditions) related to CIP except the fact that CIP specifically requires a high level of functionality in terms of dependability — including availability — and reliability. In CIP the impact of a breach in availability is crucial regardless of the origin of the failure (be it caused by a human attack or by a system - either hardware or software - failure), as the focus is more on the effect and result.

As the responsibility for IT security inside an entity is often decentralised and split between

different ‘hands’, it is difficult to arrange, ensure and justify a joint overall approach to cybersecurity ([6]). In addition, the separation of ICT security and other security issues may produce misunderstandings or uncoordinated decisions.

As ICT security is applicable and necessary across different CIP sectors, it is a relevant issue both for civilian and defence areas (called ‘dual use’). This is especially valid for the technology, although underlying procedures and environments may differ. This challenge is handled differently across the EU and a harmonised approach is still missing.

Transport

The overall transport sector is composed of different subsectors or areas of application, mainly land (railway, roads), air and offshore (maritime) with different, subsector-specific requirements and challenges. A further dimension is the distinction between passengers and goods.

The past and still the main current focus is on safety, increasingly involving security (e.g. because of terrorism) and bilateral links (‘safety-by-security’: e.g. railways, automotive, air (for both persons and goods)). Defining concrete challenges in risk awareness requires the consideration of all different specifics, possibly structured within a framework of risks. This framework should deliver an overview, taking into account the whole spectrum of risks from low probability and high impact to high probability and low impact.

With regards to legislation, an overall framework of existing or upcoming laws and regulations — on the national and European levels — would offer the basis for a qualified assessment and would support the decision-making process. The framework would need to take into account

([6]) Nowadays also defined as ‘digital security’.

interoperability and intermodality and to cover the different areas and sectors in transport. A separation is not adequate because of the intermodality required in an overall intelligent transport scheme.

As mentioned above, the current main focus in the transport sector is still on safety. But additional assessments are increasingly required related to security. Hence a comprehensive risk assessment needs to take into account both approaches. A framework dividing the detailed subsectors (road, urban transport, railways etc.) would deliver a basis for an improved risk assessment.

The assessment and testing of existing and new technical solutions requires more adequate environments and infrastructures. Simulations are one possible approach and they would require qualified data and environments. Further ones such as demonstrations and more pilots would help to enlarge and expand the experts' experience and expertise. As the whole bundle of situations and scenarios contains numerous different combinations, a 'one-size-fits-all' solution does not cover the overall challenges for operators.

The language, the viewpoint and even the understanding in the different subsectors, and particularly between the different players involved, requires some kind of 'interoperable lexicon'. Academics — responsible for research and possibly offering guidance to operators — often do not understand the (practice-oriented) needs of operators and vice versa. Such guidance may help to establish an improved common understanding and view.

During the session, participants highlighted the fact that the contribution of closed-circuit television (CCTV) as a technological solution enforcing security and improving awareness is still

under discussion because of different national legislations and cultures.

This sector differs from the others in some fundamental ways. Because of its interdisciplinary nature, transport is composed of different thematic areas (subsectors), forming a ‘cross-thematic area’. Therefore simple overall approaches are not sufficient to address operators’ needs and challenges. The current extension of the earlier (restricted) approach stressing safety aspects to include security ones, and the bilateral relationships within the area, requires a new and expanded overall approach.

Several frameworks would help to delimit the different subsectors and to improve the starting position so as to be able to perform a more qualified and adequate differentiation of specific needs. This is needed for, for example, risk assessment, but is also applicable for risk awareness and for legislation. Scenario-oriented testing, based upon pilots, demonstrations or simulations, needs better and more adequate environments, infrastructure and related conditions.

A common lexicon might ensure a better exchange of needs and offers between different parties involved (researcher vs user), for example concerning guidance to operators.

5. Report on Session 2 (Operator tools/instruments)

Driving Question for Session 2: What tools are available for operators and how can these be best utilised in order to address the above challenges regarding the assessment, selection and deployment of technological security solutions?

The operators of all three sectors (ICT, energy and transport) highlighted issues related to existing tools, how they are utilised and what is needed which is not available. The topics ranged from risk awareness to risk assessment, the security lifecycle of products, testing, evaluation, modelling, simulation and analysis (MS&A), the need for CIP education, the link between research and the marketplace, financial, regulation and legislation aspects and the need for fast and harmonised standardisation.

Energy

This sector has a strong focus on standardisation needs. Standards lack clarity and are not produced or updated quickly enough to follow the market evolution. They are often too long, do not provide clear guidance to operators and generally do not offer a framework for a prioritisation of implementing actions related to tool utilisation. Standards need to be concise, to the point, provide clear directions and be produced quickly. Current standards related to energy

focus almost exclusively on safety and not sufficiently on physical, procedural, operational or cyber security. In addition, the way tools are utilised can have a big impact on the privacy of citizens, as a lot of users' data needs to be stored and managed securely. In such a context, standards should help to strike the right balance between security and privacy. Harmonisation of standardisation is indispensable to help operators select the standards they need, and to create a fair market.

A problem related to risk assessment is how to make sure that the necessary and correct information is available to perform it. Regularly updated information is needed regarding vulnerabilities. However there is an issue of trust related to information sharing, since operators of critical infrastructures need to know about their vulnerabilities so they can address them, but in a strictly confidential way to make sure that such information does not reach a potential attacker.

There is a strong need for fully inclusive supply chain security, in order to ensure that the inclusion of new components or upgrades to existing equipment within systems or infrastructures does not introduce threats or vulnerabilities which were not originally present. It is crucial to have security assurance throughout complex systems, subsystems and components. In addition, there is a need for measures not only to protect components, but also to counterattack threats to systems that are used to control components.

More CIP education tools/mechanisms are necessary not only within the energy sector but also across sectors, in order to make sure that specialists from other sectors, or from different departments of the same sector, can understand what are the security needs of energy

operators and their specific language. A centre of excellence, academic or not, is needed to facilitate communication between the energy and ICT sectors, to improve the development of appropriate tools and to provide guidance on their utilisation. This is a generic need that does not apply only to security.

The availability of emerging technologies does not appear to be a major problem, and the information on them is easily searchable and obtainable. However, there is a lack of guidance on both their effectiveness and how to use them. This could be addressed through written guidance and demonstrations. At the same time, there is a need for intelligent and independent analysis as the proliferation of information placed on the Internet makes it increasingly difficult to select that which is valuable for the operators' needs.

Tools that are fit for purpose today might not be fit tomorrow due to changes in the environment where they are used. Therefore a lifetime analysis needs to be made about the adequacy of their utilisation, and expectations need to be managed regarding how tools will perform. More testing and evaluation mechanisms are necessary in order to provide reassurance to operators regarding the utilisation of new systems/tools. Instruments exist but some have to be improved to fit the operators' needs, and proper guidance needs to be provided for better utilisation.

Information and communication technology

An appropriate awareness of threats and related risks is indispensable for operators, and needs to be supported by adequate tools for information sharing across countries. Several technological tools exist, but they are often misunderstood by the users, who might not share the correct information. Therefore, education on the effective use of these tools is required just as much as the provision of the tools themselves. Additionally, lack of trust is an obstacle to intelligence sharing and proves that technological and human aspects need to be considered together.

Risk assessment tools exist, such as the ISO 2700x framework, and the guidance provided by the European Network and Information Security Agency (ENISA), but organisations often do not have the appropriate human skills to implement such tools correctly. The risk assessment tools often fail to take into account the dynamic aspect of cyberthreats, which evolve rapidly; standards and policies do not follow the speed of change, nor do they test the competence of an organisation. As a result, organisations compliant with standards or certification frameworks might fall into a false sense of security. Appropriate security education is clearly required in order to make sure that security staff and management understand security principles related to risk assessment and management. Another common issue is the confusion between technical risk using, for example, CVE (common vulnerabilities and exposures) scores and organisational risk, such as the impact on the business or the end user. It is necessary that the people who make decisions regarding the utilisation of risk assessment tools are accountable for their decisions.

Products and data need to be managed through the whole security lifecycle and not simply at the single test prior to deployment. The use of polymorphic and versatile tools ([7]) to assist in continuous risk assessment within a constantly changing environment appears sensible. Technologies such as autonomous intelligent agents ([8]) are already a reality, and attacks may be launched, self controlled or evolve. Research is needed to produce tools to counterattack such kind of threats. There is also a strong need for tools for MS&A of an organisation's network or overall environment, and to assist in testing/evaluation as there is currently no effective assessment MS&A available.

Hybrid simulation ([9]) tools, combining physical and abstract parts, would help towards faster and more cost-effective security evaluation exercises. Education and exercises are of paramount importance. Educational mechanisms exist but need to be strengthened and better coordinated. Operators need to communicate their operational needs to academia and research bodies. Regretfully, instruments to bridge the gap between R & D and those who design and implement the systems in an industrial environment are limited. This gap between research and market is also an obstacle to improving standardisation, which in turn needs a better harmonisation to be utilised more appropriately and efficiently.

From the financial perspective, tools should allow the end users to demonstrate a clear return on security investments. EU financial instruments such as the seventh framework programme

([7]) Polymorphic and versatile tools contain mechanisms which allow them to mutate some features (polymorphism) to adapt their functionalities to the specific scenario/environment (versatility) while keeping their original overall structure intact.

([8]) An autonomous intelligent agent is an entity which may learn, or use knowledge, to achieve its goals by observing through sensors and acting upon an environment using actuators, and by directing its activity towards achieving its goals.

([9]) Hybrid simulation is obtained through tools which combine hardware experiment with numerical simulation.

for research and technological development (FP7) exist, and also national financial support, but the issue is how funds are managed by those who benefit or deliver benefits. Regarding legislation, there are various directives within and outside the EU, as well as national plans and strategies. However, there is little in the way of national standards from a security perspective. As a result, there is no universal agreement regarding the adequacy of such plans and strategies. In addition, privacy aspects have an impact on security legislation, which needs to be taken into account in the standardisation process.

Transport

The current technical standards in the transport sector cover mainly the organisational and operational safety of the transport operators and providers, as well as infrastructure managers. However, some apply to tools such as CCTV, for example for roads and railways, which are used for both safety and security purposes. For example, in the road industry there is a common methodology of risk assessment, which focuses on the range of safety/security measures and their cost effectiveness.

European-funded projects are helping the industry in such contexts, both for providers and operators. However, even if solutions are available, there is a problem of acceptability, and of real understanding related to the acceptance of project results. That demands a serious discussion (by the European Commission, academia and industry) in regards to project dissemination and exploitation methodologies.

A consequence is the loss of good research work which could instead be used to create standards in a relatively straightforward way. In addition, more CIP education/training is needed, to help research and production of standards.

There is also a lack of availability of centralised information and visibility regarding what tools and instruments are available for operators in order to implement the best possible safety and security solutions for transport infrastructure.

It is therefore kindly suggested that the JRC might provide such a framework of CIP matters/issues for transport systems, as a sort of hub where operators would be able to share information more easily. This might help to solve the dual problems of awareness of what instruments are available on one side, and acceptance of such instruments on the other side.

Acceptance of tools would certainly need a framework in order to trigger and build a trustworthy environment among operators, with appropriate risk assessment tools that are currently not sufficiently widely and/or easily available. It is necessary to build a network of trust where information that is potentially highly sensitive could be exchanged in a secure, efficient and effective manner.

A collaborative scheme is needed in order to make sure that experts in the sector can interact in a trustworthy manner. To achieve this, an entity that would take on the role and responsibility of facilitator is strongly needed and highly recommended. Successful examples such as the European Police Office (Europol) already exist in some areas, and the JRC might want to enhance its role as facilitator for information sharing among operators.

The users of tools have a higher trust in them if related legal frameworks for their creation and utilisation exist. Regretfully, it often happens that laws are created as a reaction to major security events. This is detrimental for any sector; legal frameworks need to be put in place to prevent breaches from occurring and not after they occur.

Regarding the issue of providing guidance and support to CIP operators, simulation and training events are tools that are very much needed. It is indispensable to practise case scenarios (normally threat scenarios) on the basis of the currently available instruments in order to learn how to improve them, to understand better how to use them and to know what is missing — all in a collaborative way among operators.

This applies not only to cooperation within a sector, but among several sectors, such as the main three in this workshop, but also any others. Needless to say, this implies substantial related costs. From the financial point of view, funds exist, but there is the usual problem of who manages them and how they are used.

6. Analysis of Sessions 1 and 2 (Overall operator challenges)

While several challenges are common to all sectors, not all of them have the same relevance and importance. As a result, feedback and recommendations coming from one sector need to be handled very carefully before applying them to other sectors, as 'one-size-fits-all' solutions are not suitable. This appears to be particularly relevant to the **energy** sector due to its specific framework (e.g. global approach). In the **transport** sector the main focus is on safety rather than security. Safety and quality have to be taken into account as complementary elements and linked to security. The **ICT** sector strongly needs the entire supply chain to be secured dynamically, down to the individual component. This main concern is shared by all operators, as ICT has a direct impact on any other CI sector due to the need for, and deployment of, ICT components and systems. Most of the following issues are broadly common to all sectors, and most likely also to CI sectors not represented in this workshop.

Challenges in risk awareness vary from the absence of guidance for proper education and training to the need for better, clearer and more concise standards. CIP education is essential and needs to be strengthened. Operators of CIs need information about European and national research results, as well as ongoing research projects, in order to aware of emerging technologies, validation results concerning existing technologies and gaps in innovation which need to be communicated to the managers of research programmes. Training programmes need to be harmonised at the EU level and related certification schemes established for operators' staff. There is a need to support such efforts through relevant professional education and training/research budgets. ERNCIP can help create efficient and effective bidirectional communication between operators and research bodies, and link the relevant stakeholders

within the standardisation community to ensure standards are created rapidly and effectively.

Operators need a political contribution to encourage input from research and innovation, as well as for operational matters. European harmonised procedures and legislations are necessary to improve coordination at the European and global levels, and to ensure a common level of security-related requirements and fair financial burden for the operators' business. A major challenge consists in measuring and estimating risks, as well as calculating or estimating costs. Scenario-oriented approaches, related but not limited to risk assessment, would enable a more structured process, as would new models for risk and costs estimation. Financing and related investments are challenges which have a direct impact on the business, and hence on competiveness.

Information sharing regarding threats and vulnerabilities, as well as available/needed tools and instruments, is still a huge challenge because of a missing central reliable point of trust. An external facilitator would help build trust among operators; ERNICP might want to play an important role in this respect. Also in terms of regulation policies, ERNCIP can help in communication among operators aiming at requesting DH Home Affairs to coordinate its CIP policy areas with those in other policy areas. It is stressed that at national level politicians need strategy, management boards need regulations and technicians need reference manuals for appropriate guidance on the assessment, selection and deployment of technological security solutions. There is also a need to create an EU-wide auditing scheme for operators of critical infrastructures, based on a harmonised methodology.

7. Recommendations from Session 3 (ERNCIP's role at EU level)

Driving Question for Session 3: How can the ERNCIP network help to address these challenges on an EU level?

The participants welcomed this meeting, underlining their appreciation that ERNCIP is listening to the problems and needs of operators of critical infrastructures and inviting it to consider organising such events more often. From an operator's point of view, upcoming meetings should result in more specific concrete statements and recommendations for actions.

It was pointed out that the staffing resources of operators are limited. As a consequence, participation in such meetings will be driven by an assessment of how valuable they can be for the organisation. ERNCIP should build on the very positive feedback from this meeting and launch a systematic outreach initiative to operators. This might include information meetings at national level facilitated by authorities in the Member States.

Overall, while recognising the amplitude of its efforts, ERNCIP was asked to leverage its role to a higher level of facilitator in all the areas described in this report.

Recommendations addressed to policymakers

Operators need a political contribution to encourage input from research and innovation, as well as for operational matters. Procedures and legislation that are harmonised at the European level are necessary to improve coordination at the European and global level, and to ensure a common level of security-related requirements and a fair financial burden for the operators' business. A major challenge consists in measuring and estimating risks, as well as calculating or estimating costs. Scenario-oriented approaches, related but not limited to risk assessment, would enable a more structured process, as would new models for risk and costs estimation. Financing and related investments are challenges which have a direct impact on the business, and hence on competiveness.

With regards to legislation, an overall framework of existing or upcoming laws and regulations — on national and European levels — would offer the basis for a qualified assessment and would support the decision-making process. During the workshop this request was particularly well illustrated in the transport sector. Here the framework would need to take into account interoperability and intermodality and to cover the different areas and sectors in transport. A separation would not be a good solution because of the intermodality related to a required overall intelligent transport scheme.

Based on the presentation of ERNCIP, it appears that, from an operators' point of view, the existing thematic areas are scattered and an umbrella structure reflecting the sectorial relevance is missing. Hence, within the current framework of theoretical areas, the big picture of critical infrastructure protection might be missing or incomplete. As a result, participants invite

the service of the European Commission in charge of ERNCIP to identify new thematic areas more related to the overall theme of CIP. Specifically, participants proposed the establishment of new thematic areas within a sectorial context.

This process should be executed in close collaboration with operators. ERNCIP should establish these new thematic areas by breaking down selected complex infrastructures ('disaggregation from the big picture'). The list of new areas should include, but not be limited to, topics like:

- the MS&A of security vulnerability identification, assessment and optimisation and the evaluation of security solutions, interdependencies, etc.;
- human factors and security culture;
- the threat landscape in energy, in particular the cybersecurity of smart grids and renewable energy.

Furthermore, the operators underline the need to link security with existing safety efforts. One example is **safeurity** — a concept being developed within the rail sector addressing the interdependencies establish a comprehensive protection of infrastructures and operations — of any kind.

The participants pointed out that no EU-wide harmonised training for operators exists, nor does a certification of qualified personnel. The participating operators asked ERNCIP to facilitate the creation of such an EU-wide harmonised training scheme for operator staff. The repository of threats and vulnerabilities of CIs, as previously requested, should be used for these training sessions.

As part of the same process, consideration of the implementation of an EU-wide security certification of qualified staff is also requested. (This would allow the experts to work at different CIs throughout the EU, and make it easier for the owners of the CIs to recruit staff.) The resulting extra costs should be included in Erasmus+[10] or equivalent education budget lines of the EU.

Participants also underlined that the proposed training schemes should be addressed to senior staff (engineers as well as managers). At the same time the creation of curricula for critical infrastructure protection at university level was also requested. (NB: This request is in line with the obligations and mandate of the Academic Committee of ERNCIP. The ERNCIP office is asked to keep both operators and academia informed and to facilitate a related brainstorming between them.)

Participants recommended that ERNCIP establish a database of incidents, which should be updated on a weekly base. Such a central tool (as a single point of reference) would allow operators to be informed about potential threats in an effective and timely manner.

In the same context, operators invited ERNCIP to launch a systematic assessment of past events like the earthquake in Haiti, Hurricane Katrina in New Orleans and the Gulf coast of the United States and the tsunami damage to the Fukushima nuclear plant in Japan, with a focus on the interdependencies of different critical infrastructure sectors (e. g. energy, communication, transportation, water supply) and cascade effects.

10 The EU programme for education, training, youth and sport (http://ec.europa.eu/programmes/erasmus-plus/index_en.htm)

Participants discussed various threats from terrorist attacks to natural hazards, and from those of high probability and potentially low impact to those of low probability but potentially high impact. It was underlined that the probability may be perceived as less important in comparison to the consequences of failures of components of complex systems or sectors of CIs. Hence guidance is requested regarding risks of low probability but potentially high impact, as in such scenarios operators may risk ignoring the unavailability of critical services (e.g. lack of energy due to extreme space weather, which would result in an inability to manage water supply). ERNCIP might want to consider providing guidance or an information framework to help operators prevent such kind of occurrences.

There was common agreement among participants that exercises on a national and EU-wide scale, based on common threat scenarios, would be needed. ERNCIP is invited to facilitate such exercises.

Regarding the need for MS&A of CIP, it is a common understanding that CIs are complex systems with interdependencies across various sectors (e.g. the well-reported energy–water–food nexus).

Based on the assessment of past events and monitoring of threats to CIs reported worldwide, MS&A efforts could drive the development of scenarios to be used for analysing possible cascade effects.

Recommendations aimed at the research community

Operators feel that there is not enough information available about security research efforts at EU as well as at national level. At best, only promotional types of leaflets are available, for example at the CORDIS website of the EU. It is highly desirable to receive an overview of what has been sponsored so far in research in the context of CIP at EU level as well as at national level. In particular, operators would like to be informed about the research results, the impact of these projects and how the results achieved will be exploited to increase the security of CIs.

Participants invited ERNCIP to facilitate the production of this information and a dialogue between the managers of the research programmes and CI operators. By doing so, gaps and needs for further research can be established and the innovation process, the core of Horizon 2020, can be promoted.

A significant part of the discussion was related to the risk assessment of CIs. The term 'risk' has been used in the sense given by Frank H. Knight ([11]), and is different to uncertainty. However, risk is not easily measurable, like the length of a table, particularly if it concerns rare events. Risk definition and assessment have to be reconsidered to ensure all those involved are speaking the same language. (with reference to ISO 31000 of 2009 and ISO Guide 73 of 2009).

It has been suggested that risk assessment and subsequent risk management be structured

([11]) In 1921, Frank H. Knight published a book entitled *Risk, Uncertainty and Profit* (published by Houghton Mifflin Company, Boston and New York) which became one of the most influential economic texts providing the theoretical basis of the entrepreneurial American economy during the post-industrial area. He drew a sharp distinction between risk and true uncertainty.

into questions like the following:

- What are the means to provide security?
- Which technologies are in use? Are they proven? Are they used elsewhere?

Building a comprehensive risk picture should include:

- unwanted events: TAHOI (technical failure, acts of god, human error, organisational weaknesses — including level of legislation — and intentional acts — from internal threats to war);
- relevant objectives at stake (availability, financial effects, human lives, i.e. the safety objectives);
- looking at all dimensions: BITOP (buildings' physical infrastructures, information, technical systems (ICT, organisational artefacts (structure + procedure and people));
- being modelled in a 'societal model' like the one used for MNE7 — multinational experiment 7 — to be used as a platform for the comprehensive exercise of developed test scenarios/use of cases developed.

Recommendations aimed at the ERNCIP project

It is commonly agreed that it is difficult to validate models in a statistically significant approach. However, ERNCIP is about the testing of security solutions. Therefore it is recommended to use such models to disaggregate complex systems (security solutions) in order to identify components for testing and validating — and subsequent aggregation of the results in order to validate the overall system.

This aspect relates to a further topic which has been discussed, namely the need to involve actively the ERNCIP network of test facilities. There is an urgent need to establish common test methodologies and test protocols for security solutions. (It should be noted that this is even part of the ERNCIP mission statement.) Perhaps a better term than testing could be evaluation of security solutions. The ERNCIP office is invited to establish a dialogue with the laboratory network and operators of CIs to discuss such methodologies — not only in laboratories but also in the 'real field'. In this context, in particular, collaboration with ETSI (European Telecommunications Standards Institute) will be instrumental.

Regarding the presentation of ERNCIP, it appears that, from an operators' point of view, the existing thematic areas are scattered and an umbrella structure reflecting the sectorial relevance is missing.

Workshop website

https://erncip-project.jrc.ec.europa.eu/

How to contact ERNCIP

Carl-Johan Forsberg

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen
Security Technology Assessment Unit
Via E. Fermi, 274921027 Ispra (VA), Italy

E-mail: erncip-office@jrc.ec.europa.eu

Tel. +39 0332 786628
Fax +39 0332 786565

European Commission
EUR 26858 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Second ERNCIP Operators Workshop - Workshop report

Authors: Klaus Keus, Carmine Rizzo, Alois J. Sieber

2014 – 44 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-42602-5

doi:10.2788/17555

Abstract

In order to intensify the collaboration with operators of critical infrastructure, ERNCIP has so far organised two cross-sectoral Operators' Workshops; the first one took place in Brussels on 12-13 September, 2013 and the second one took place in Ispra on 19-20 May 2014. This document is co-written by the three moderators for the second Operators' Workshop; Carmine Rizzo, Klaus Keus and Alois J. Sieber. The report summarises and analyses the discussions and also presents some recommendations based on the outcome.

LB-NA-26858-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Publications Office

doi:10.2788/17555
ISBN 978-92 -79-42602-5