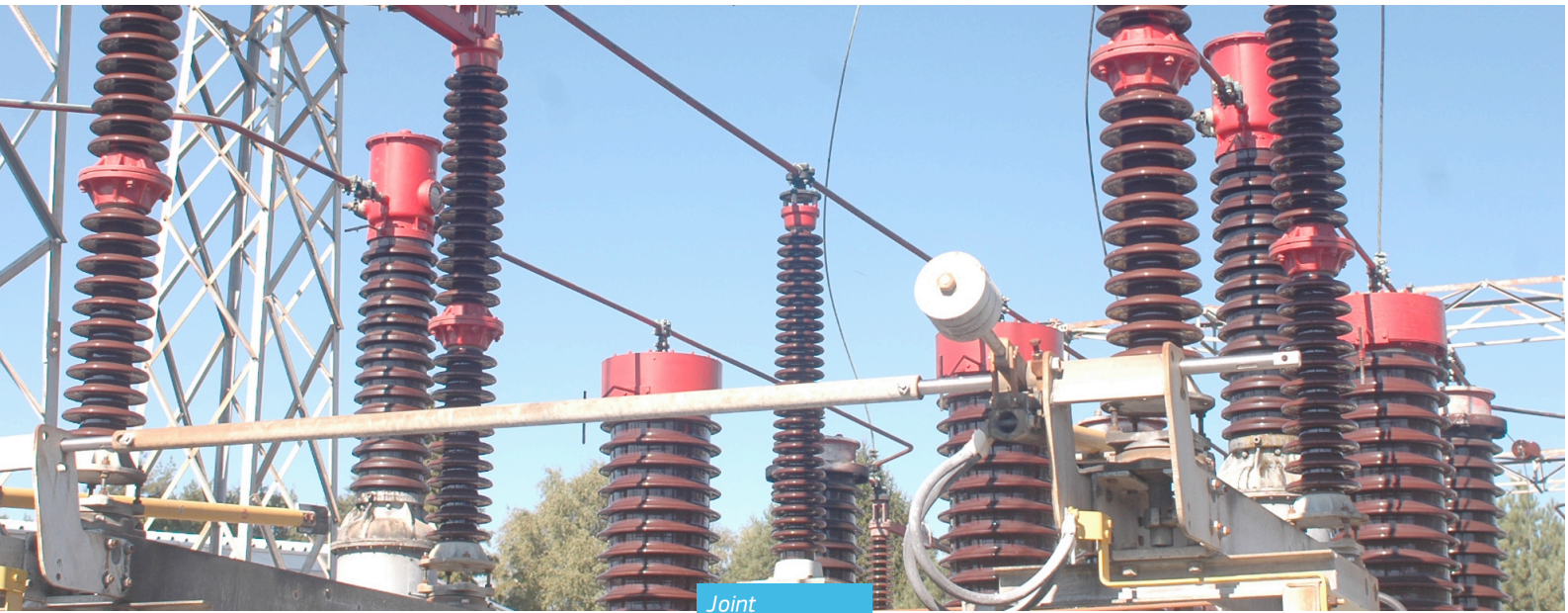
European Commission

JRC SCIENTIFIC AND POLICY REPORTS

European CIP-related Testing Capabilities: Gaps and Challenges

Christer PURSIAINEN
Peter GATTINESI

August 2013



Joint Research Centre

Report EUR 26229 EN

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

Contact information
Naouma Kourti
Joint Research Centre, Via Enrico Fermi 2749, TP 720, 21027 Ispra (VA), Italy
E-mail: Naouma.Kourti@ec.europa.eu
Tel.: +39 0332 78 6045
Fax: +39 0332 78 6565

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

JRC85192

EUR 26229 EN

ISBN 978-92-79-33760-4

ISSN 1831-9424

doi:10.2788/34627

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

EUROPEAN REFERENCE NETWORK for CRITICAL INFRASTRUCTURE PROTECTION (ERNCIP)

European CIP-Related Testing Capabilities: Gaps and Challenges

Authors:

Christer PURSIAINEN
Peter GATTINESI

The authors would like to particularly acknowledge the contributions of the ERNCIP Thematic Group coordinators and members, and other respondents who have provided valuable views and information. The sole responsibility of the correctness of the information presented lies with the authors.

August 2013

Contents

Glossary

The following terms are used in this report, based on their ISO definitions[1]:

Accreditation is the formal recognition by an independent body, generally known as an accreditation body that a certification body is capable of carrying out certification.

Certification means the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.

Conformity assessment is the process used to show that a product, service or system meets specified requirements.

A **standard** is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.

Testing is the determination of one or more of an object or product's characteristics and is usually performed by a laboratory.

Other common terms used within this paper are:

Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

Security refers to protection against threats by terrorism, serious and organized cross-border crime, natural disasters, pandemics and major technical accidents.

[1] http://www.iso.org/iso/home/ (NB all hyperlinks referenced in this paper were last accessed on 9 Aug 2013).

Abbreviations

^{3}He	Helium -3; a light, non-radioactive isotope of helium with two protons and one neutron
AESA	Agencia Estatal de Seguridad Aérea (Spanish Aviation Safety and Security Agency)
ALMERA	Analytical Laboratories for the Measurement of Environmental Radioactivity
CBRNE	Chemical. Biological, Radiological, Nuclear, Explosives
CEA	Commissariat à l'énergie atomique et aux énergies alternatives (French Alternative Energies and Atomic Energy Commission)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEP	Common Evaluation Process
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CTM	Common Testing Methodology
DG	Directorate-General
DOVO	Dienst voor Opruiming en Vernietiging van Ontploffingstuigen (Belgian Explosive Ordnance Disposal)
ECAC	European Civil Aviation Conference
ECI	European Critical Infrastructure
EDS	Explosives Detection System
EMI	Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, (Germany)
ENEA	Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)
ENISA	European Network for Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ERNCIP	European reference Network for Critical Infrastructure Protection
EURATOM	European Atomic Energy Community
EU	European Union
FOI	Totalförsvarets forskningsinstitut (Swedish Defence Research Agency)
FP7	EU's Seventh Framework Programme for Research
GC-MS	Gas chromatography coupled to mass spectrometry
GC-MS-MS	Gas chromatography - tandem mass spectrometry
HR	High resolution
IACS	Industrial Automation and Control Systems
IAEA	International Atomic Energy Agency
ICP-MS	Inductively coupled plasma mass spectrometry
ICS	Industrial Control Systems
ICT	Information and Communication technology
ICT	Fraunhofer Institute for Chemical Technology (Germany)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITRAP+10	Illicit Trafficking Radiological Assessment Programme+10
ITU	Institute for Transuranium Elements (of the JRC)
JRC	Joint Research Centre (of the EU)

LC-MS-MS	Liquid chromatography - tandem mass spectrometry
LEDS	Liquid Explosives Detection System
NESDE, LNEC	Earthquake Engineering Division, National Laboratory for Civil Engineering (Portugal)
PPP	Public-private partnership
RN	Radiological and nuclear
RTD	Research and Technological Development
SCADA	Supervisory Control and Data Acquisition
SecurEau	Security and decontamination of drinking water distribution systems following a deliberate contamination (FP7 project)
SERIES	Seismic Engineering Research Infrastructure for European Synergies (FP7 project)
SPIRIT	Support of Public and Industrial Research Using Ion Beam Technology (FP7 project)
SSc	Security Scanners
SWD	Staff Working Document
SWOT	Strengths, Weaknesses, Opportunities, Threats
TAMARIS	European Facility for Advanced Seismic Testing (France)
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (Dutch Organization for Applied Scientific Research)
TREES Lab	Laboratory for Training and Research in Earthquake Engineering and Seismology (Italy)
TSA	Transportation Security Administration (US)
VÚPCH	Research Institute of Industrial Chemistry (Czech Republic)

List of Figures and Tables

Executive summary

The Institute for the Protection and the Security of the Citizen of the Joint Research Centre (JRC) of the European Commission set up the European Reference Network for Critical Infrastructure Protection (ERNCIP) project in 2009. This took place under the mandate of the DG Home, and with the agreement of Member States. The project is due to complete at the end of 2014.

One of ERNCIP's goals is to identify gaps in European CIP-related experimental and testing capabilities, and to set up a wider debate on how to deal with these gaps. This report draws an indicative picture about the known state of European CIP-related test capabilities. The analysis is primarily based on an ERNCIP online questionnaire on the issue circulated at the end of 2012, which was completed by 65 respondents representing different types of ERNCIP stakeholders. The ERNCIP Thematic Groups have also provided information about their respective capabilities and perceived gaps in their sectors. This report aims to provoke further debate among the ERNCIP stakeholder communities.

In some sectors, the EU has impressive CIP-related testing capabilities, although there still appears to be a lack of some capabilities. However, there is no detailed picture available about the existing capabilities, and even less about specific gaps. Instead, CIP stakeholders tend to make reference to general impressions about the absence of European capabilities, in terms of know-how and infrastructure. The reason for this uncertainty may be that European-level test capabilities are connected to European standards, the absence of which makes it difficult to identify the requirements for test facilities, and therefore difficult to identify the testing infrastructure gaps in the EU. This also explains why there is no horizontal, cross-sectoral European-level plan to enhance test capabilities.

For the way forward, the report recommends adoption by the EU of an overarching policy to improve CIP by enhancing related security solution testing capabilities, based on an approach which combines selectively building up test capabilities in the EU, while enhancing cooperation with non-EU experimental facilities and test laboratories. Under this high-level policy, sector/thematic-level activities will enable a focussed approach towards European testing capability building, coordinated with the on-going process of creating, harmonising and validating European security standards.

Specifically, this report proposes that the methods and processes to implement this policy are further developed in the future work of ERNCIP. A multi-stakeholder ERNCIP workshop in 2014

should be arranged with the aim to agree on and prioritise the areas where gaps in test capabilities are perceived to prevail. Additional ERNCIP Thematic Group(s), representing all relevant stakeholders, would then be formed to identify and evaluate the specific capability gaps and development challenges in the prioritised sectors, considering the criticality, costs and other factors. These thematic groups would analyse the different options for meeting the capability gaps, including EU-led and/or EU–funded approaches, Member State–based approaches, market-based approaches, and combinations thereof. The aim of these groups would be to produce detailed recommendations to the relevant funding and implementation bodies, including the respective EU policy areas, so that specific policy conclusions can be articulated in the relevant EU policy.

1 INTRODUCTION

1.1 Background – what is ERNCIP?

The Institute for the Protection and the Security of the Citizen of the Joint Research Centre of the European Commission set up ERNCIP in 2009. This took place under the mandate of the DG Home, in the context of the European Programme for Critical Infrastructure Protection (EPCIP),[2] and with the agreement of Member States. The preparatory phase was successfully completed in November 2010 and the project started its implementation phase in February 2011.

The definition for 'critical infrastructure' within the EPCIP context states that critical infrastructure "means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[3] As with EPCIP, the general objective of ERNCIP is to improve the protection of critical infrastructures in the EU, both critical national infrastructure, as well as the subset defined as European Critical Infrastructure.[4] ERNCIP works in close cooperation with all CIP stakeholders, focusing particularly on the technical protective security solutions.

The mission of ERNCIP is - "*To foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities"*. In order to achieve this, ERNCIP puts its efforts into maintaining an online inventory of CIP-related experimental capabilities in Europe, and into developing a network of experts to identify and promote good test practices to form the basis of common European testing standards, aiming at harmonisation of test methodologies and test protocols, where practical.

[2] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm.
[3] *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, p. L 345/77.
[4] While EPCIP's scope includes also supporting the protection of national critical infrastructures in wider sense, the EPCIP Directive focuses only on European critical infrastructures and concentrates on the energy and transport sectors, where the 'Europeanness' is defined as follows: "'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States."

One of ERNCIP's goals is to identify gaps in European CIP-related experimental and testing capabilities, and to set up a wider debate on how to deal with them.[5] ERNCIP's starting assumption is that EU self-sufficiency in all aspects of testing for CIP-related security applications cannot be justified, but that the EU could continue to rely on world-wide collaboration.[6] However, it is sensible for the EU to consider whether there are any CIP-related areas where EU self-sufficiency in testing capabilities is desirable and achievable, and also whether there are areas where closer cooperation with non-EU capabilities would bring greater value.

1.2 Structure of the report

This report aims to consolidate known information, and provides the basis to provoke further debate among ERNCIP stakeholders, with the issues presented in five sections. First, the issue of test capabilities is set into a wider context, assessing, on the basis of publicly available material, the main challenges for the EU security industry in a global perspective.

One way of identifying the challenges in terms of missing European testing capabilities is to identify when European actors use, or are even dependent on, the services of non-EU facilities and laboratories. However, while there is a general understanding that the EU-US relationship is quite active in CIP, including EU-located actors' use of US experimental facilities and laboratories for testing security solutions, there is virtually no open-source data about the extent and nature of this cooperation. Therefore, the ERNCIP Office prepared a questionnaire to survey this aspect with its stakeholders, which has provided some general views on this issue. The second section of this report discusses the results, covering where and why European actors cooperate with non-EU experimental facilities and laboratories.

Third, on the basis of both the ERNCIP survey and the information provided by the ERNCIP Thematic Groups, a comprehensive picture is presented about the current state of European CIP-related test capabilities. Again, while the available information is only indicative and not based on exhaustive data-gathering or analysis (one recommendation is for a more systematic approach to collect such data), some gaps in EU capabilities are apparent. The section also illustrates some of the activities underway that aim to fill these gaps.

[5] *ERNCIP Roadmap 2010*. This goal is detailed in WP6 ('Self-sufficiency'), pp. 95, 96.
[6] *ERNCIP Roadmap 2010*. WP11 ('International collaboration'), pp. 104, 105.

Fourth, SWOT analyses of alternative ways of meeting the needs for CIP-related testing capabilities are presented, covering the status quo, a more proactive approach to increase EU self-sufficiency in security testing capabilities, enhanced international cooperation, and a combined approach. This section also suggests a basic methodology of how to prioritise between different needs to increase self-sufficiency of EU capabilities.

Finally, the paper summarises the main (tentative) conclusions and recommendations, and proposes a general framework for further analysis and decision-making on these issues.

2 SETTING THE CONTEXT

Setting the context is important because the notion of experimental and testing capabilities, in terms of expertise and infrastructure, is not an isolated issue and cannot be dealt with properly without also discussing related issues, such as the status of European security industry, the level of product standardization, the absence of common testing methodologies across the EU in many fields, and the absence of mutually recognized certification schemes across the EU.

2.1 Global security market dominated by the US

Drawing on existing market report estimates and consultation with industry representatives, the 2009 ECORYS review[7], on which the 2012 Commission staff working paper[8] backing the recent EU Security Industrial Policy Communication[9] is largely based, estimates that the global "security market" is worth some €100bn. A more recent market analysis focuses on "the CIP market" instead, which forms a smaller sub-market of "the security market". This 2013 MarketsandMarkets analysis expects CIP investments to increase across the globe, with the expected market to grow from €50 bn in 2013 to €82 bn by 2018.[10]

According to the ECORYS 2009 review, the US constitutes the world's largest market for security with around 41% share, as illustrated in Figure 1; the EU comes next with around 25%, well ahead of China, Japan, Israel and Russia. The review expects the market to grow at a

[7] ECORYS (et al 2009), *Study on the Competitiveness of the EU security industry*. Within the Framework Contract for Sectoral Competitiveness Studies – ENTR/06/054, Final Report, Brussels, 15 November 2009: http://ec.europa.eu/enterprise/policies/security/files/study_on_the_competitiveness_of_the_eu_security_industry_en.pdf. The sectors covered are, except the last one, basically the same as the ERNCIP is dealing with currently: air transport of goods (cargo); maritime transport of goods (cargo); CBRNE; biometrics; secure communications; protective clothing.

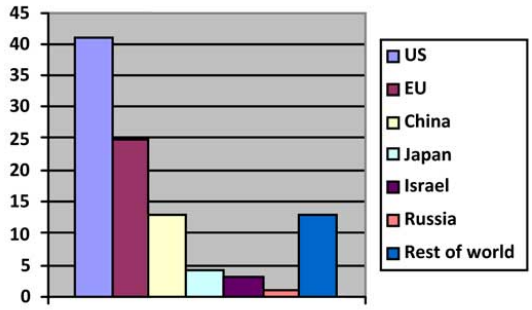
[8] Commission Staff Working Paper, *Security Industrial Policy. Accompanying the document, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Security Industrial Policy. Action Plan for an innovative and competitive Security Industry*, Brussels, 26.7.2012 SWD(2012) 233 final. COM(2012) 417 final: http://ec.europa.eu/enterprise/policies/security/files/commission_staff_working_paper_-_security_industrial_policy_-_com(2012)_417_final_en.pdf.

[9] Communication from The Commission to the European Parliament, the Council and the European Economic and Social Committee. *Security Industrial Policy. Action Plan for an innovative and competitive Security Industry*, Brussels, 26.7.2012. SWD(2012) 233 final. COM(2012) 417 final: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF.

[10] MarketsandMarkets : http://www.marketsandmarkets.com/Market-Reports/critical-infrastructure-protection-cip-market-988.html. The figures in the text above are converted; in original, $63.76 billion in 2013 to $105.95 billion by 2018, at a Compounded Annual Growth Rate of 10.7%. The report furthermore states the following: "The energy and transportation sector are highly prone to these effects because of the increasing levels of dependence on the information communication technologies or the information infrastructure. CIP other than energy and transport has a wide portfolio of applications across manufacturing and chemical industry, sensitive infrastructures such as stadiums, government facilities, manufacturing, banking facilities, historical monuments, holy places and defense establishments."

minimum of 5% per annum, with the fastest growth in coming years taking place mainly in Asia and the Middle-East.

Figure 1: Global market shares for security (%)



As a result of the inconsistent basis for these market analyses, it is difficult to draw firm conclusions about the comparative shares of sales achieved by the security industry according to country; however it is mentioned in the ECORYS review that the US companies cover over 45% of the global export in safety and security equipment.[11]

In any case, it is generally perceived that the EU is clearly behind the US in this industrial sector, in terms of size, volume, competitiveness, and, perhaps, innovation.

2.2 A need to develop EU security standards

As early as 2004, the *Research for a Secure Europe* report, produced by the high-level 'Group of Personalities' tasked with developing the EU security research programme, noted that in the field of security equipment and solutions:

- the US is taking a lead;
- that US technology will progressively impose normative and operational standards worldwide; and
- in certain areas, where the US authorities prioritize their investment and achieve fast product 'speed to market', that the US will enjoy a competitive advantage.[12]

[11] ECORYS (et al 2009), p. 48. The figures are based on a US Security Industry Association figures from 2006.
[12] *Research for a Secure Europe* (2004). Report of the Group of Personalities in the field of Security Research. Rapporteur Burkard Schmitt: http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf.

The 2009 ECORYS review further concluded that while the EU has a great potential in the security industry, it does not utilize its possibilities through harmonizing and creating a more coherent European regulatory environment; thus the EU is failing to provide the necessary level of clarity required by industry to make investment decisions. In contrast to the EU, the US government, it is argued, is both more demanding (in regulation) and more accommodating (with federal funding programmes) in terms of technological requirements, pushing technology forward proactively, and by so doing also creating an environment that is more attractive for companies to invest in security technology development. It is further claimed in the ECORYS review that by developing a national system for standardization, tailored for the US needs, the US has created *de facto* unilaterally defined global security standards, which further enhances the US dominance of the field. Consequently the review recommended enhancing the EU-level standardization framework in the security field, especially in those sectors where there is absence of standards or where the standards differ across Member States.

The 2011 ECORYS review on security regulations[13] similarly concluded that a more harmonized European regulatory framework would provide the potential to enhance the competitiveness of the EU security industry, particularly by reducing the current fragmentation of EU markets, which is said to hamper the development of the industry, and makes security more expensive for customers.

Indeed, following these recommendations, work towards more harmonized European regulatory frameworks and standards is currently taking shape in the field of security, encouraged by the developing EU Security Industrial Policy. In particular, this is taking place within the CEN/CENELEC framework under Mandate M/487 on security standards, where security refers to protection against threats by terrorism, serious and organized cross-border crime, natural disasters, pandemics and major technical accidents.[14] ERNCIP and its Thematic Groups have been, and continue to be, facilitators and participants in activities on these priorities, especially those dealing with CBRNE threats, and the application of biometrics for CIP.

[13] ECORYS (et al 2011), *Security Regulation, Conformity Assessment & Certification*. Final Report – Volume I: Main Report, Brussels, October 2011: http://ec.europa.eu/enterprise/policies/security/files/doc/secerca_final_report_volume__1_main_report_en.pdf.

[14] *Programming Mandate Addressed to CEN, CENELEC and the European Telecommunications Standards Institute to Establish Security Standards, M/487,* EN, Brussels, 17th February 2011: ftp://ftp.cencenelec.eu/CENELEC/EuropeanMandates/M_487.pdf.

2.3 A need for European testing and certification schemes

Commonly-agreed international or EU standards are a prerequisite to developing common EU test methods, simply because if there is no agreed-upon performance standard against which one should test, it is difficult to agree upon a common test methodology. Harmonization of standards should be accompanied by a mechanism for mutual recognition across the EU of products certified at national level, thus improving the regulative framework and infrastructure for validating and certifying security products.

European manufacturers are particularly concerned that the current systems are costly, time-consuming and unpredictable. While there are some tangible examples that overcome these shortcomings,[15] this is not the general case. It is argued by manufacturers and vendors of security solutions that, instead of forcing them to test and certify the security products separately for 28 markets in national testing facilities and laboratories, each following their own testing methodologies and requirements, it should be possible to agree upon European common test methodologies. When certification is needed and practical, mutually recognized certification schemes should be agreed. In this context, the following comment from the ERNCIP survey is relevant:

> *"There is a significant variation between test labs, in terms of testing methodology, and results for the same tests we would expect to be the same, are not. There are very significant differences in terms of prerequisites and documentation required to start the tests. Duration of and urgency to get test done differs enormously with significant ramifications for vendors - not being able to sell to markets for a whole quarter or missing out on tenders." (Vendor)*

Manufacturers, vendors and others using EU-based test laboratories have also indicated that conformity assessment and certification bodies often have a near monopoly position in their respective Member States. Finding this situation unsatisfactory, the users call for increased competition for the provision of certification services; the assumption is that a harmonized and mutually recognized certification system in the EU would reduce the cost and raise the quality and professionalism of provided services.[16]

Ideally, it should be sufficient for a security product to be tested in one accredited European test laboratory in order to have access to the EU single market. This would also indirectly enhance the

[15] For instance, the Illicit trafficking radiation assessment programme (ITRAP+10) run by the JRC and funded by DG ECHO.

[16] ECORYS (et al 2011), *op. cit.,* p. 216.

competitiveness of European security industry in its export efforts if the European standards and certification schemes were to become more generally recognized.

To sum up, further development of the European security industry presupposes an improved EU-level testing and certification scheme with enhanced approval and certification infrastructure either by creating a new one or harmonizing the existing national ones.

3 EU RELIANCE ON NON-EU CAPABILITIES

The goal to further develop the European security industry, together with more harmonized standards, testing methodologies and certification schemes, implies the need for sufficient expertise, capability and capacity of experimental and testing facilities in Europe. How do we know whether this sufficiency exists, and how can we identify where the gaps are? One way to approach this issue is to ask: "to what extent are the EU-based actors (manufacturers, operators, government agencies, testing facilities etc.) cooperating with, using, or even dependent on, the services of non-EU testing facilities and laboratories, and why?"

While there is no database or open-source information to definitively answer these questions, some general trends in this respect are revealed by the ERNCIP survey. The survey was made between September and December 2012 through an anonymous, mostly online, multi-choice questionnaire, which also allowed for detailed free text contributions. The questionnaire was completed by 65 respondents representing different types of ERNCIP stakeholders, which can be considered as a satisfactory response.[17] The main results are presented in this section.

3.1 Widespread and regular international cooperation

In general, the EU is open and positive towards international cooperation in the field of CIP.[18] The use by EU-located organisations of non-EU experimental facilities is part of this cooperation.

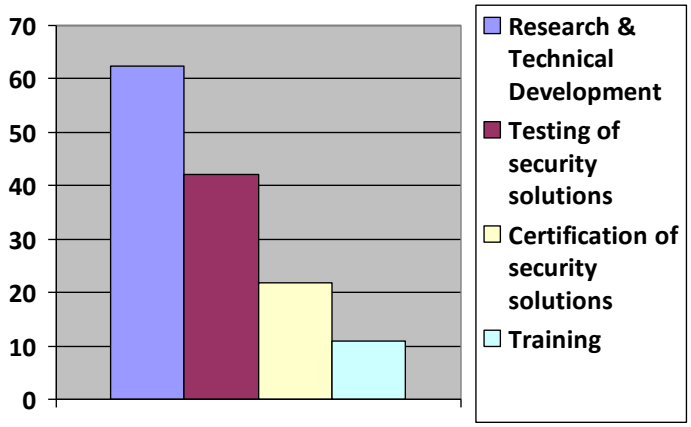
[17] In order to maximize the participation, the questionnaire was designed to be as simple as possible. Note that only some general views can be identified on this basis, and it cannot be understood as statistically valid. Experimental facilities and laboratories made up of around 39% of the responders, followed by manufacturers or vendors with 25%, national competent authorities with almost 19%, national certification organizations or regulators with around 9.5% and CI operators with just 3% of the responders.

[18] There is a 2011 'Council Conclusions on the development of the external dimension of the European Programme for Critical Infrastructure Protection', which invite the Member States to step up cooperation with relevant third countries. In the EC documents, one usually categorizes the third countries into several categories. 1) The EEA countries (Norway, Iceland, and Liechtenstein), which are invited to all EPCIP-related meetings. 2) The United States and Canada, with whom the EU has bi- or trilateral CIP-focused meetings on rather regular basis as well as sub-sectoral working groups. Some individual Member States also refer to their bilateral (Germany, Poland, and Sweden) on-going or intended cooperation with the US, sometimes based on agreements, and in the case of Sweden, also including Canada.3) Russia is mentioned especially by Germany, those two countries having a multiannual bilateral agreement including CIP cooperation. Several other countries have expressed their interest in enhancing CIP cooperation with Russia, in particular on energy. 4) China is also mentioned by Germany referring to training in CIP-related matters.5) Israel has also cooperation with Germany on bilateral basis. 6) Multilateral cooperation takes place between the EU countries and other international organizations, most notably with the North Atlantic Treaty Organization, and the Organization for Security and Co-operation in Europe. See: Commission Staff Working Document, *Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, Brussels, 22.6.2012, SWD(2012) 190 final: http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf.

The ERNCIP survey shows that EU actors use non-EU experimental facilities for testing and certification in the field of CIP applications for a variety of purposes, as illustrated in Figure 2.

About two thirds of respondents to the ERNCIP survey regularly cooperate with non-EU experimental facilities in the field of Research & Technological Development (RTD) and about a tenth cooperate for training. This type of cooperation is not surprising for European experimental facilities and laboratories (representing the majority among the respondents in general), but many manufacturers, vendors, and operators of CI also participate in RTD or training cooperation.

Figure 2: For what purposes do organisations cooperate regularly with non-EU experimental facilities in testing and certification? (%, n=65)



According to the survey, around two thirds of respondents favour development of further cooperation with non-EU experimental facilities, and call for a more enhanced European approach to support this cooperation, as will be discussed below in more detail. The same message comes frequently and directly from ERNCIP stakeholders in the Thematic Group meetings and this was also the general spirit in the ERNCIP Conference in December 2012. Cooperation with US-based experimental and testing facilities, which are considered to be better equipped and more advanced in their capabilities, is especially appreciated as a way to enhance expertise.

The survey does not show any specific CI sector where this type of cooperation is more common, nor does it suggest the forms of funding programmes under which this cooperation takes place. In practice, several forms of cooperation are likely. We know that in the field of radiological and nuclear security there is a well-established cooperation between the EU and the US Department of Energy. More generally, there is the EU-US expert cooperation in CIP, started in 2010,

although this cooperation has yet to establish any formal framework, especially on CIP-related RTD and training cooperation. European manufacturers often cooperate with US test facilities to enable sale of their products in the US.

When it comes to pure research, the FP7 Framework Programme (in the next funding period known as Horizon 2020) is the flagship for European research cooperation. While security research had been excluded in EU framework programmes before 2007, it was included from the beginning of FP7. In terms of cooperation with non-EU countries, FP7 allows, within specific funding schemes and rules depending on the country, strategic partnerships and project cooperation with third countries, including those playing a major role in the security industry.[19] RTD cooperation with the US has been a celebrated special case within the FP7 framework programme: "Transatlantic science and technology collaboration is very well developed and US participation represents 11% of the total non-European participation in FP7 so far. The success rate of US research teams winning bids is high, comparable to the success rate of many EU-based entities."[20] In general, there is a high-level political commitment to enhance the EU-US scientific and technological cooperation. Security as a field of cooperation, however, is not among the top fields in this EU-US cooperation, though there are some individual examples.[21]

To contribute to this cooperation, the JRC in general (e.g. within ITRAP+10 programme[22]) and ERNCIP more specifically, has especially developed its relations with the National Institute for Standards and Technology[23], which is a federal technology agency of the US Department of Commerce that works with US industry to develop and apply technology, measurements, and standards. While this JRC/NIST cooperation has so far been limited to exchange of information, it should serve as the basis for more developed exchange programmes and RTD, especially in the field of CIP.

[19] http://cordis.europa.eu/fp7/who_en.html#countries. For the major cooperation countries in CIP for the EU, see footnote 18.

[20] *Transatlantic Cooperation in the European Seventh Framework Programme for Research & Development. A Guide for U.S. Users. A resource for researchers and institutions in the USA to build transatlantic partnerships under the FP7 Cooperation Programme*, p. 3: http://www.eurunion.org/FP7-USGuide-12-09.pdf.

[21] As an example of US participation in the field of security is the 'European network for the Security of Control and Real-Time Systems': http://cordis.europa.eu/projects/rcn/87538_en.html.

[22] http://www.dhs.gov/illicit-trafficking-radiological-assessment-program-10-itrap10.

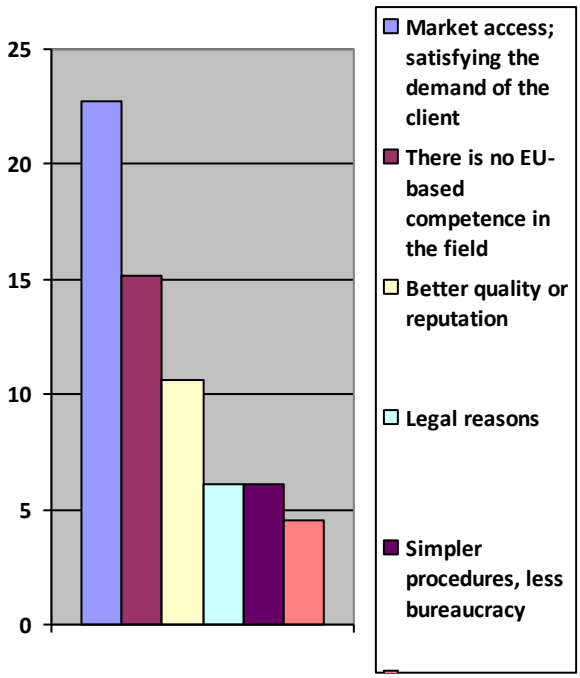
[23] http://www.nist.gov/homeland-security-portal.cfm.

3.2 Why do EU actors test and certificate in non-EU facilities?

As Figure 2 also shows, about half of the respondents to the ERNCIP survey informed that they *regularly* test or certify security solutions in non-EU experimental facilities. Most of those respondents who test security solutions outside the EU are manufacturers, vendors, or CI operators, with a few national competent authorities or regulators.

As Figure 3 illustrates, in many cases this testing takes place simply because the manufacturers or vendors need to test and receive a certificate in that non-EU country in order to access that country's market. Thus, around a quarter of the respondents to the ERNCIP survey use non-EU facilities regularly in order to get access to markets, or to satisfy the demand of the client. In comparison, the legal or regulatory requirements of non-EU countries were identified by only six per cent of respondents.

Figure 3: Why do EU actors rely on non-EU experimental facilities? (%, n=65)



However, the survey also informs that European actors rely on non-European, mainly US experimental facilities to test products that are aimed at European markets, too. This may refer to cases where test results and certificates, especially from the US, are accepted within the EU in lieu of any specific European standards or certifications. An interesting fact is that about 16% of the respondents to the ERNCIP survey use non-EU facilities regularly because there is no competence in a particular field in Europe. This response and the related free text information

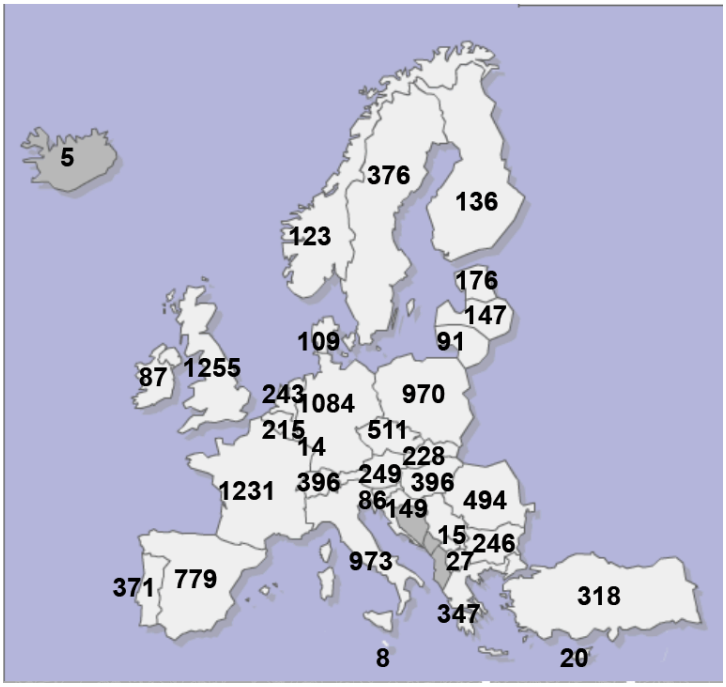
indicate clear gaps in European testing capabilities (discussed further in the next section). For about a tenth of the respondents, better quality is the reason to regularly use non-EU experimental facilities.

The conclusion from the study of the ERNCIP survey results is that cooperation with the US and other countries' experimental laboratories and testing facilities is appreciated by ERNCIP stakeholders. This cooperation, particularly in RTD and training should be enhanced with further coordinated programmes in order to build up the expertise of European test capabilities in CIP-related security solutions.

4 WHERE ARE THE GAPS IN EUROPEAN TESTING CAPABILITIES?

It is a difficult task to identify the gaps in European testing capabilities in the field of CIP-related security solutions in any detail. It is almost as difficult to get detailed data about the existing capabilities, except country-by-country or by individual laboratories. Comprehensive data does exist at national level about the accredited laboratories, certification, and inspection and verification bodies, collected by the national accreditation bodies, and organised European-wide by the European Cooperation of Accreditation, partially available on their website.[24] In fact, there are several thousand accredited laboratories in the EU, with several hundred in many Member States, as illustrated in Figure 4.

Figure 4: Accredited laboratories in the EU



Source: Paolo Bianco's presentation at the 1st ERNCIP Conference in December 2012. Figures are based on a 2011 survey. Following ISO/IEC 17025 (General requirements for the competence of testing and calibration laboratories).

However, to specifically single out the CIP-related capabilities is difficult. The ERNCIP Inventory[25] aims at filling this information gap, collecting detailed profiles of CIP-related testing facilities and laboratories. This Inventory is increasing its data population, reaching about 100 facilities by August 2013. However, it has proved difficult to get some types of laboratories to participate, especially those within the private sector used for in-house testing only, as they see little benefit from advertising their expertise more widely. In any case, by definition, the ERNCIP

[24] http://www.european-accreditation.org/ea-members.
[25] https://erncip.jrc.ec.europa.eu/.

Inventory does not identify gaps, but lists assets. Consequently, it is not possible to draw a holistic picture, either within a sector or across sectors, of the gaps in EU testing capabilities. Furthermore, the lack of product performance standards and test standards makes it difficult to define what infrastructure and other capabilities are needed.[26] Nevertheless, this section draws a rough picture about the existing CIP-related capabilities in the EU in those sectors where ERNCIP is currently active as well as tentatively identifying the fields where gaps exist.

4.1 Sectors lacking European testing capabilities

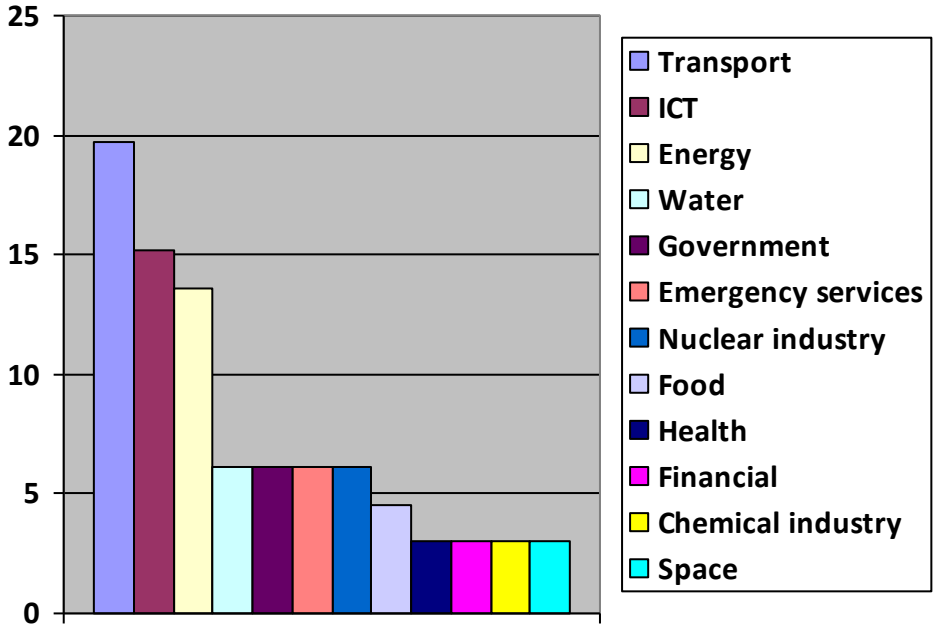
When asked in the ERNCIP survey which specific CI sectors are most clearly lacking in terms of testing capability and/or quality in the EU (see Figure 5 below), the top three candidates were transport, ICT and energy, with comment made on specific issues of smart grids, explosives detection and resistance to explosive effects. Other sectors were mentioned by a few respondents.

Typical free text comments in the context of this question are e.g.:

> *"There are few European facilities for testing new devices related to security item, in particular for explosive and biohazard materials." (Experimental facility or laboratory)*
>
> *"The current problem in testing to meet regulatory approval is the lack of facilities or expertise." (Manufacturer or vendor in security industry)*
>
> *"The capability of EU explosives ranges is limited and it has been necessary to use facilities with larger explosive limits in non-EU countries." (Competent government authority)*
>
> *"There is a lack in testing facilities on home-made explosives including characterization, effects and detection of explosives." (Experimental facility or laboratory)*
>
> *"I am not aware of any EU testing facilities that are capable of manufacturing/ handling/manipulating large quantities of explosives, particularly sensitive explosives such as home-made explosives." (Competent government authority)*
>
> *"In my field, there is a government-funded organization [in the US] that does testing on a scale which no individual EU Member State could afford." (Competent government authority)*
>
> *"I am always amazed, when, looking at the test report [of a US facility instead of a EU facility], I see what tests they have done." (Manufacturer or vendor in security industry)*
>
> *"More often than not, it is the experience of the personnel rather than the infrastructure that is the barrier to having capability". (Competent government authority)*

[26] There are, of course, exceptions. For instance, this has been defined within ITRAP+10 in the Border Monitoring Radiation Detection Equipment field.

Figure 5: In which sectors is the lack of European capability most obvious? (%, n= 65)



4.2 Gaps in testing identified in the ERNCIP Thematic Areas

This section takes a closer look at the current state of the art of experimental and testing capabilities by analysing each field where ERNCIP is actively involved. ERNCIP has established networks of experts in nine prioritised thematic areas, which focus on specific risks to critical infrastructure in these areas (i.e. explosives detection in aviation and non-aviation sectors, industrial control systems, seismic risks against structures, explosive effects against structures, chemical and biological risks in water, video analytics and surveillance, applied biometrics to CIP, and radiological and nuclear risks to CI).[27] By analysing the testing capabilities in each of the nine ERNCIP thematic areas in detail, different approaches to meeting the gaps are tentatively identified.

[27] For details of these thematic areas, see: Peter Gattinesi and Christer Pursiainen, *European Reference Networks for Critical Infrastructure Protection: Thematic Areas. State of the Art.* Available in the European Commission PUBSY JRC82093, May 2013.
http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/29088/1/lbna26017enn.pdf

4.2.1 Aviation security detection equipment

Existing capabilities

In common with all the thematic areas, gaps in the testing capabilities required for aviation security will be the consequence of the need to test security solutions against the standards that are defined for such security solutions.

There are EU regulations in place to define the basic standards for aviation security.[28] In addition, the European Civil Aviation Conference (ECAC)[29] has developed a testing process for aviation security equipment, the ECAC Common Evaluation Process (CEP[30]). This process is based on an ECAC agreed Common Testing Methodology (CTM). ECAC CTMs currently exist for Explosive Detection System (EDS), Liquid Explosive Detection System (LEDS) and Security Scanners (SSc). The ECAC CTMs are endorsed by all 44 ECAC member states (which includes EU-28), but they are not legally binding.

Test centres made available by national authorities in ECAC member states have been approved by ECAC to evaluate the performance of EDS, LEDS and SSc, with the results of these evaluations transmitted to all ECAC member states. However, these test centres are not formally recognised by the European Commission, as is the case with notified bodies[31] in the single market legislation[32]. Only a few EU Member States currently have ECAC-approved testing centres; France, Germany, Spain, the Netherlands and the UK. In addition, Switzerland operates a test facility.

[28] The main European regulatory framework, in full effect from 29 April 2010, is laid down by Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002: http://ec.europa.eu/transport/modes/air/security/.

[29] https://www.ecac-ceac.org//activities/security.

[30] CEP represents a harmonised evaluation of different categories of security equipment, and provides Member States with robust and reliable information on their performance against set technical specifications.

[31] Certification, inspection or testing body designated by the Notifying authority of a EU Member State to perform the Attestation of Conformity of products within the scope of a New Approach Directive. Member States may add requirements for the bodies they notify. Additional requirements can be accreditation, participation in European co-operation, restrictions on subcontracting etc.: http://ec.europa.eu/enterprise/newapproach/nando/index.cfm?fuseaction=glossary.main.

[32] "Notified bodies carry out the tasks pertaining to the conformity assessment procedures referred to in the applicable technical harmonisation legislation when a third party is required. […] The primary task of a notified body is to provide services for conformity assessment under the conditions set out in the directives." http://ec.europa.eu/enterprise/policies/single-market-goods/internal-market-for-products/conformity-assessment-notified-bodies/index_en.htm#h2-2.

More generally, there are about a dozen test facilities in Europe that deal with explosive detection (see Table 1 in section 4.2.2). Not all test centres offer all three types of ECAC CEP tests, and other national aviation security testing may occur at the test centres, for example on Explosives Trace Detection (ETD). An important additional part of testing of aviation security equipment is operational trial at airports. Such trials and their results have to be reported to the Regulator (DG MOVE).

Gaps and challenges

While some of the EU laboratories are well equipped and match other aviation security laboratories like the US Department of Homeland Security's Transportation Security Administration (TSA) test centres, the main difference is that the TSA is a US federal authority establishment, whereas all the facilities in the EU are national.

That there are too few test centres, implying that not all stakeholders or Member States have sufficient access to them, is perceived as a possible test infrastructure gap. The ECORYS 2011 study, which informed the EU's work on the Security Industrial Policy, remarked: "Also noticeable is the limited scale of the infrastructure for undertaking testing of these categories of security technologies: […] in the aviation sector, under ECAC CEP there are only 4 test centres for Explosive Detection Systems (EDS) and 3 centres for Liquid Explosive Detection Systems (LEDS)."[33]

Possible solutions and approaches

The JRC is creating an aviation security laboratory to provide an in-house capability for the European Commission, scheduled to open in early 2014. It is hoped that this laboratory will be made available also to experts from the EU Member States. The concept is that the laboratory should allow relevant stakeholders who currently do not have access to well-equipped laboratories to get hands-on experience to study, for example, performance of detection equipment, minimum detection requirements, measurement standards and simulants.

The EU work on the Security Industrial Policy, including a harmonised certification system, with accredited test centres, might increase the availability of aviation security test centres, as laboratories additional to the current ECAC-approved test centres could also be eligible to

[33] ECORYS (et al 2011), *Security Regulation, Conformity Assessment & Certification*. Final Report – Volume I: Main Report, Brussels, October 2011, p. 19: http://ec.europa.eu/enterprise/policies/security/files/doc/secerca_final_report_volume__1_main_report_en.pdf.

participate as a test centre. Some of the test centres listed in Table 1 are also increasing their test capabilities as part of their natural development, as new regulations are enforced and new equipment enters the market.

4.2.2 Explosives detection equipment (non-aviation)

Existing capabilities

Experimental work in explosive detection is linked to the national regulations on handling explosives, especially home-made explosives, which limits the number of laboratories involved in this area. The actual detection testing is not the only aspect to be considered for testing of explosives detection equipment. Other aspects include synthesis (preparation of explosives), characterization, and the safe storage of explosive products, which can be extremely dangerous in some cases. There are only a few European laboratories that have experimental facilities that can work on explosives detection (especially outside aviation). Table 1 (below) provides the known (not necessarily comprehensive) list of facilities where explosives detection can be tested in Europe.

Gaps and Challenges

The main concerns in this field are more related to the lack of regulations and standards in a non-aviation context, rather than lack of testing infrastructure. Several laboratories are working on trace detection but no common protocols exist for the evaluation and certification of trace detectors. The first studies in the field are in progress in the context of ECAC, but these are only aimed at aviation security. Outside this area, no work has been started. Furthermore, the generation of samples (particles, vapours) is crucial in this field. For instance, CEA[34] and Fraunhofer ICT[35] have capabilities for calibrated gas generation. However, before we can identify any testing capability gaps in explosive trace detection, more work is needed at EU level to identify the need for common standards or guidelines in this area.

[34] CEA is a French government-funded technological research organisation: http://www.cea.fr/english-portal.

[35] The Fraunhofer Institute for Chemical Technology: http://www.ict.fraunhofer.de/en.html.

Table 1: The known European testing capabilities in explosives detection

Location	Test Centre	Capability
Belgium	DOVO	
Czech Republic	VÚPCH	
France	CEA	Can test all kind of detection technologies. Can synthetize and handle home-made explosives.
France	Service technique de l'aviation civile	EDS
Germany	Federal Police Technology Centre/ tests done at Fraunhofer Institute (ICT)	EDS, LEDS, SSc Can synthetize and handle home-made explosives.
Italy	ENEA	Limited explosives types and quantities.
Netherlands	TNO, Defence, Security and Safety	EDS, LEDS, SSc Can synthetize and handle home-made explosives.
Spain	AESA	SSc
Switzerland	Armasuisse	LEDS No synthesis facilities.
Sweden	FOI	Can synthetize and handle home-made explosives.
UK	Centre for Applied Science and Technology	SSc
UK	Defence Science & Technology Laboratory	Can synthetize and handle home-made explosives

Possible solutions and approaches

For explosive trace detection, the ECAC common testing methodology in progress for aviation security will be a good basis for the testing of security solutions to meet any similar requirements outside aviation security, for which the ERNCIP Explosives Detection Equipment (non-Aviation) Thematic Group is contributing to the analysis. As already mentioned, JRC is building a laboratory for the evaluation of different detection technologies which will also be used outside aviation applications.

4.2.3 Industrial automation and control systems

Existing capabilities

The EU Cybersecurity Strategy from 2013 takes up part of the issue discussed in this report, noting that there is "a risk that Europe not only becomes excessively dependent on ICT[36] produced elsewhere, but also on security solutions developed outside its frontiers." While the strategy does not explicitly discuss testing, by strongly promoting a European single market for

[36] Information & Communication Technology.

cyber security products, it implies the need for improving European test capability and adopting harmonized testing methods.[37]

What then is the situation for Industrial (Automation and) Control Systems (IACS or ICS), for which Supervisory Control and Data Acquisition (SCADA) systems are the largest subgroup, used to monitor and control critical infrastructure?

A recognized problem in this area is that while there are many standards for SCADA systems, there is a lack of agreement on which standards are to be used Europe-wide. In practice, from a manufacturer's point of view, customers refer to many different standards and requirements, which results in extra costs; the industry has therefore been arguing for a clearer understanding of what are the minimum requirements for SCADA security in the EU.

There has also been much discussion on whether a European certification scheme would be needed to ensure a common minimum level of security. For SCADA systems this is however a complicated and controversial issue, due to, inter-alia, the fact that the systems are continually updated with new software, and in order to test security, both the individual components and the whole system have to be tested. Repeated certification becomes too costly and time-consuming.

Whether or not a common certification scheme is needed, SCADA systems have to be security tested. Currently the manufacturers, vendors and in some cases also operators do most of the testing in their own facilities, or they use specialized test services and laboratories, often working globally. Some of the major test laboratories are US-based.

Gaps and challenges

The current ICS/SCADA tests are conducted on several levels, usually including at least the component, subsystem and whole system levels. However, what cannot be tested easily, and what is not usually therefore tested at all in Europe, is the system-of-systems level, including interoperability with other systems and possible failure propagation and cascading effects due to unpredicted or complex interdependencies (e.g. physical/cyber interdependencies between a gas pipeline, an electricity grid and the related SCADA systems).[38]

[37] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN(2013) 1 final, p. 12: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

[38] See: Irene Eusgeld, Cen Nan and Sven Dietz, 'System-of-systems'' approach for interdependent critical infrastructures', *Reliability Engineering and System Safety,* Volume 96, Issue 6, June 2011, pp. 679–686.

These interdependencies are difficult to model and simulate, but even more difficult to test in an operational environment. While there are some ICT cyber security test facilities in Europe, they cannot be used in their current form to fully test the security of ICS because it is not possible to perform actual operational tests with the ICS connected to actual critical infrastructures. Unlike in the US, there are no testing facilities in Europe which can connect ICS to infrastructure, such as an electricity grid (instead of relying on simulated tests). How the ICS/SCADA security tests are exactly conducted by the manufacturers and vendors, be it in Europe or in the US, is not transparent however, as these actors are reluctant to detail their test methodologies on the basis of competitive advantage.

Perhaps partly for this reason, a fundamental question, which has been around for a long time, is whether there should be a more 'independent' European test bed for SCADA systems, separate from manufacturers' and vendors' in-house testing.[39] Recently the EU-agency European Network for Information Security (ENISA) raised this issue in the context of ICS. [40]

Possible solutions and approaches

ENISA is the main driving force within the EU that is identifying the problems related to SCADA/IACS testing. ENISA's current approach is that Europe has to make a choice between two alternatives. Either the EU should create a common test bed at European level based on a Public-Private Partnership, aiming at "conducting independent verification and validation tests […] in a controlled environment, ensuring integrity and increasing the trustfulness on certified/tested solutions. Moreover it will provide operators with independent security evaluations and a common security reference so that they are supported when deciding which products/services to buy." Alternatively, ENISA proposes, the EU should create a common ICS security certification framework based on the Member States' existing certification systems and, possibly, a European coordination group to avoid duplicated work so that "once a product is certified in a Member State's national laboratories, it wouldn't be necessary to certify it once again."[41] This implies that the testing capabilities of the Member States' national laboratories would need to be harmonised/upgraded to the required level.

[39] E.g. Henrik Christiansson and Eric Luiijf, 'Creating a European SCADA Security Testbed', *Critical Infrastructure Protection, IFIP International Federation for Information Processing* Volume 253, 2007, pp. 237-247.
[40] ENISA, *Protecting Industrial Control Systems Recommendations for Europe and Member States* [Deliverable – 2011-12-09], Recommendation #5, p. 45: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.
[41] Ibid.

Currently, a report, based on a survey among the different stakeholders, is being prepared by ENISA to continue the discussion on which of these alternatives the EU should opt for.

4.2.4 Structural resistance against seismic risks

Existing capabilities

An existing FP7 project, SERIES (which also provides the core of the ERNCIP Thematic Group in this field) has gathered together 24 partners, and includes all the key actors and capabilities in Europe's seismic engineering research, including seven world-class seismic testing centres, listed in Table 2 below.

Table 2: Main European seismic engineering experimental capabilities

Location	Test centre	Capability
Nantes, France	IFSTTAR (ex-LCPC)	Centrifuge facility
Saclay, France	TAMARIS, CEA	EU's largest 6-degree-of-freedom (6DoF) Shaking table
Pavia, Italy	TREES Lab, EUCENTRE	EU's largest Uniaxial Shaking Table and Bearings Tester
Ispra, Italy	European Laboratory for Structural Assessment, JRC	EU's largest reaction wall & Power Spectral Density lab
Lisbon, Portugal	NESDE, LNEC	Large 3DoF Shaking table
Bristol, UK	BLADE, University of Bristol	6DoF earthquake Shaking table
Cambridge, UK	University of Cambridge	Centrifuge facility

Gaps and challenges

SERIES resulted from its initiators acknowledging that there are some gaps in European seismic engineering capabilities, and that European seismic engineering is lagging behind the US, Japan and increasingly also the Chinese capabilities. Existing capabilities in Europe are unevenly distributed: there are European countries with high seismicity but no research infrastructures, and countries with large research infrastructures but low seismicity. There is an unused potential in Europe for the scientific and technical community to pursue promising research ideas, because of lack of access to research infrastructure.

Possible solutions and approaches

To resolve the identified gaps, the SERIES project was established as a capacity and capability building project, aiming at enhancing the European capabilities in experimental seismic

engineering by better integration of existing capability. The two main ways SERIES is enhancing European capabilities are:

- Implementation and maintenance of a Distributed Database of test results, which allows the research community to get access to a huge amount of data from earlier research.
- Through the FP7 project funding (to be ended in 2013), a peer review system which provides a free-of-charge access to the European test centres, listed in Table 2, to those EU countries, companies, research facilities lacking of experimental capabilities but having an experimental need.

4.2.5 Resistance of structures against explosion effects

Existing capabilities

There are three different types of testing methods applicable for blast resistance testing: a) direct high-explosive testing, b) shock tube testing, c) and numerical simulations. Around Europe only a very limited number of experimental facilities and laboratories deal with the structural resistance of constructions against explosives threats.

The key players in this field are all included in the ERNCIP Thematic Group, as listed in Table 3 below; beside these, only some small laboratories deal with the topic (e.g. Spiez in Switzerland). These smaller laboratories usually have testing facilities for only fundamental laboratory tests like the Hopkinson Pressure Bar, which is able to determine the dynamic resistance of concrete, but cannot directly test the resistance against explosion.

Table 3: Main European experimental capabilities dealing with structural resistance against explosives

Location	Test centre	Capability		
		Direct high explosives test	Shock tube test	Numerical simulation
Germany	Technical Centre(s) of the German Armed Forces (WTD)	X	X	X
Germany	Federal Institute for Materials Research and Testing (BAM)	X		X
Germany	Fraunhofer Institute (EMI)	X (scaled experiments)	X	X
UK	GL Noble Denton, Spadeadam	X		
France	CEA, Gramat	X (scaled experiments)		X
Netherlands	TNO		X	X
Finland	Technical Research Centre of Finland (VTT)			X
EC	JRC			X

Gaps and challenges

The information from the ERNCIP survey indicates that there are gaps in explosive-related experimental and testing capabilities in the EU, especially from the limitations in the amount of explosive. On the other hand, the information from the ERNCIP Thematic Group indicates that it is not the experimental capacities that are missing, but that the regulative framework to conduct these kinds of tests for critical infrastructure is absent. There are no regulations that bind the operator of a critical infrastructure to consider the resistance of against explosive threats. As long as such testing is purely voluntary, most operators will not test against these threats, since this will cost money. In respect to blast resistance of buildings, international standards exist only for the test and classification of glazing used in buildings.

Possible solutions and approaches

This ERNCIP Thematic Group aims at addressing the regulative gap, by creating the basis for harmonized and comparable test methodologies. In addition, there are FP7 projects (e.g. SPIRIT[42]) which also address the security of constructions against explosive threats.

4.2.6 Chemical and biological risks in the water sector

Existing capabilities

In general, organisational structures and scientific methods today provide a high-level control mechanism for environmental water resources and for drinking water. First, there exist national accredited laboratories in all EU countries to test water quality. Second, well-developed European regulatory frameworks also exist to protect environmental water resources from pollution and to guarantee a good chemical and ecological status of environmental water resources, as well as to set quality standards for drinking water at the tap. The European regulations define rather carefully the normal substances permitted in drinking water as well as the list of pollutants, such as heavy metals, and their acceptable limits.

The current system is however designed for long-term decision making and not for immediate response in case of an incident. Generally, laboratories of the drinking water companies specialise in routine analysis, which does not require special equipment that involves high costs for their acquisition and specialized personnel. The number of parameters analysed by such laboratories is established in accordance with the requirements of the legislation and only in few cases do they perform research activity for developing analytical methods for other possible pollutants. Water

[42] http://www.spirit-ion.eu/Project.html

operators and authorities are not interested in analytical methods for substances which are not included in regulations or EU Directives and this is one of the reasons why laboratories are not stimulated to develop such methods. For this reason they cannot perform a rapid investigation of unknown pollutants to respond to an unexpected event.

However, innovative water quality monitoring systems have been developed in the last couple of years which allow for real-time control of the overall water quality. These systems react to a number of classes of contaminants and can immediately warn operators and decision makers of potential contamination in the network. Classical analytical approaches are then needed in order to identify and quantify individual chemical or biological contaminants that are the cause of a change in water quality.

Gaps and challenges

Incident response can be divided into two challenges. Real-time monitoring of water quality in drinking water networks is the first challenge, working as an early-warning system. Several tools have been developed to identify the water quality in the event of an incident. However, there is no EU standard approach that sets out the assessment parameters, for real-time monitoring of drinking water (raw water, blended water etc.) which would help to avoid false alarms and ensure that the sensors are working properly.

This lack of a standard approach is mirrored by the lack of relevant test capabilities in the existing laboratories. Several studies provide information on testing procedures or report testing of sensors and their suitability as early warning system. However a common testing guideline is missing which would facilitate placing sensors/early warning systems on the European market by setting out the relevant procedures, and the pollutants to be tested. Testing sensors in real water treatment systems is usually impossible, and simulated or laboratory tests cannot easily replicate the real environment. To test these types of early warning systems, sensors need to be placed in artificial water networks, so that the water can be spiked with different chemicals/pathogens, and the response evaluated. This will require a laboratory-scale drinking water network(s) to be created in Europe. However, such facilities would be costly, and in any case would be restricted to testing only with defined pollutants.

Screening methods for the rapid analytical identification and quantification of unknown hazards (biological and chemical pollutants) are the other challenge for incident response. Qualitative screening for hazards does not necessarily need special instruments, as this can be carried out by standard equipment which is commonly used in testing laboratories. However, the broad

application of screening is limited, as there is not a wide market for this purpose and therefore screening methods are not normally used in routine testing programs.

More thorough investigation can be done by laboratories from research institutes and national authorities which are well equipped with most of the equipment necessary for performing screening analysis of unknown substances,[43] have personnel with a high level of expertise in this field, and which develop new methods of analysis for different types of organic pollutants, in the frame of research projects. On the other hand, most of the results of research activity remain unknown to standardization bodies, to regulatory authorities and even to water operators who can only obtain such information from published articles or in conferences.

Therefore, in order to deliver valid and robust (and all-embracing) results, screening methods have to be established and laboratories have to continually deal with these methods, which in turn requires a market for this purpose. Molecular techniques such as polymerase chain reaction provide sensitive, rapid and quantitative analyses for a number of pathogens (including emerging strains) and are applied by a number of laboratories in Europe to evaluate the microbiological quality of water by facilitating identification, genotyping, enumeration and pathogens viability. Again, this technique requires experience and refinement to be applicable to a diversity of matrixes, and hence a high throughput of samples.

European expertise in the analysis of non-targeted compounds in water exists in only a few EU Member States (especially Germany, Spain, the Netherlands), and in Switzerland.[44] "Unknown" contaminants are a challenge because a high number of chemicals have to be taken into account and special screening methods have to be applied to identify substances, although chemical and physical characteristics do limit the number of possible chemicals that might be a threat to water networks.

[43] To illustrate, for instance, in Romania alone, there are 128 accredited laboratories having as profile of activity analytical investigation of water quality. From these, 82 laboratories perform routine or temporary analytical control of drinking water (laboratories from drinking water companies, from public health authority and water authority, research institutes and private laboratories). Laboratories which belong to national authorities and research institutes combine analytical investigations with development of new testing methods which is why they have modern equipment like: gas chromatography coupled to mass spectrometry (GC-MS, all of them) , gas chromatography - tandem mass spectrometry (GC-MS-MS), High resolution (HR-) liquid chromatography - tandem mass spectrometry (LC-MS-MS) for identification of unknown organic pollutants (screening analysis) and also for quantitative analysis; inductively coupled plasma mass spectrometry (ICP-MS, for metal identification and quantification). Approximately seven laboratories from Romania have such expertise.

[44] This conclusion was drawn in a literature study undertaken by the ERNCIP TG on Chemical and Biological Risk to the Water Sector: Sara Rodriguez-Mozaz and Marta Llorca, *State-of-the-art of screening methods for the rapid identification of chemicals in drinking water.* To be published on the ERNCIP website in September 2013.

Besides conventional molecular techniques, a promising approach for monitoring drinking water pathogens is nanomaterial-enabled biosensors. However, although a range of sensors have been developed, the suitability of these assays for whole-cell and microorganism detection in environmental samples has typically not been established.

Possible solutions and approaches

As discussed above, the issue here is that while testing is obligatory for several substances, it is not for many toxic substances, even if this is now possible through available methods, equipment and know-how. Part of the problem is the missing standards, but also that the necessary expertise is not developed where the testing is not part of routine testing.

Biological and chemical risks in drinking water are within the scope of the CEN/CENELEC mandate to develop security standards. Simultaneously, there are also several projects and networks underway, which also deal with the above mentioned issues, or parts of them. Beside the ERNCIP Thematic Group, dedicated to reviewing the existing practices and providing guidelines for testing new technologies, the FP7 project SecurEau, for instance, dealt with security and rapid decontamination of drinking water distribution systems following a deliberate contamination,[45] and FP7 project SIPE is promoting and increasing the use of existing research results in support of further standardization.[46]

In terms of testing infrastructure, there are also on-going national projects to build up artificial water networks, which would enable the testing of the instruments and methods for early warning for contaminated drinking water.

4.2.7 Video analytics and surveillance & applied biometrics

In the case of emerging technologies such as video surveillance and biometrics in the context of CIP, the main issue is whether there exist sufficient quality datasets against which the commercial security applications can be tested. While no comprehensive picture exists of the availability of datasets across the EU Member States, individual Member States and institutions, especially in the UK, France and Germany, have considerable capabilities to this effect.

[45] See the project's website: http://www.secureau.eu/index.php?id=3.
[46] See the project's website: http://www.sipe-rtd.eu/ .

Thus, there are methods, literature and datasets for the event detection scenarios available for the evaluation, testing, and validation of commercially available video analytics systems, and there exists a wide range of user guidance documents intended to help users develop effective CCTV systems for security applications.[47] In biometrics, too, some datasets exist that are used to test and compare the applications.

The "European problem" here is that the datasets are not standardised between countries or test facilities, so that a system tested in one country is not necessarily tested with the same parameters in another country. A related issue is that due to the nature of the content of these datasets, there are inhibitors to sharing the datasets for privacy or other legal reasons. One possible solution might be to share the datasets on a metadata level which would make it possible to establish a more harmonised test methodology in the EU within these fields.

4.2.8 Radiological and nuclear threats to critical infrastructures

Existing capabilities

There are many experimental facilities and test laboratories in the field of radiological and nuclear (RN) risks in the EU. The main database listing these is the IAEA-administrated ALMERA network (Analytical Laboratories for the Measurement of Environmental Radioactivity), established in 1995, which is a cooperative effort of analytical laboratories world-wide.[48] Members of ALMERA are nominated by their respective IAEA Member States as laboratories that would be expected to provide continuous, reliable and timely analysis of environmental samples, according to EURATOM Treaty articles 35 and 36, including in the event of an accidental or intentional release of radioactivity. Currently ALMERA consists of 128 laboratories representing 81 countries, including 66 European laboratories.

There are, however, only a few laboratories that have the capabilities and capacities for testing and qualifying technologies and methodologies related to RN security. In Europe, the JRC has been entrusted by the European Commission to set up a dedicated facility for testing the technology used for the detection and the identification of RN materials.

[47] See, for instance, examples from the UK and France: http://www.homeoffice.gov.uk/science-research/hosdb/i-lids/; http://www-sop.inria.fr/members/Francois.Bremond/topicsText/etiseoProject.html; http://www-sop.inria.fr/members/Slawomir.Bak/gpEasy/DataSet.
[48] http://nucleus.iaea.org/rpst/ReferenceProducts/ALMERA/ALMERA_Member_Laboratories/index.htm.

Gaps and challenges

Technological development, combined with threats arising from security rather than safety concerns, are bringing about new challenges and also new gaps in experimental and testing capabilities. In many applications, spectrometers are replacing counters as radiation detectors. As an example, during security missions with a task to detect radioactivity, the background gamma-ray count-rate of the detector changes continuously. Only the spectrometer is able to tell whether the observed variation is caused by the naturally-occurring radionuclides or by artificially-produced radionuclides used in malicious acts.

For stand-off detection exercises (source-to-detector distance >10 m),[49] important from the security point of view, high-activity sources are required. However, institutes typically have few, if any, high-activity sources in-house. Obtaining them comes with the obligation of secure storage, handling, bookkeeping etc. Moving them between institutes is probably less feasible than organizing tests in the source owner institute. Organizing stand-off-detection tests in other organizations usually requires a lot of effort, planning and good-will. There are also several materials such as weapons-grade plutonium or highly enriched uranium that are not commercially available in large quantities. Other than for national work by the larger EU nuclear countries, tests with these materials need to be organized at the JRC's nuclear security unit, the Institute for Transuranium Elements (ITU) in Karlsruhe, Germany.

Another complication related to security-driven testing is that often either the source or the detector needs to be moved in a controlled manner. In addition to tests with unshielded sources, different types of evasive (shielding, masking) scenarios should also be considered. For example, the shape of the energy spectrum changes if shielding is introduced. Different types of source shields should be designed and built in advance to allow the controlled and comprehensive performance evaluation of the detectors. Detectors used in safety and security also need to be tested at high radiation levels, and therefore their dynamic range of operation has to be well characterized. Moreover, factors such as insensitivity of gamma detectors to neutrons, and vice versa, need to be experimentally examined.

^{3}He counters are very common neutron detectors. The required ^{3}He is a side-product of nuclear weapons fabrication. Diminished production of nuclear weapons and increased demand of neutron detectors (e.g. homeland security projects) has boosted the research and development of

[49] For nuclear/radiological security, the location of the source is often unknown, and therefore exercises will use comparatively long source-to-detector distances.

alternative ways to detect neutrons. Both direct and indirect techniques are actively being studied. Testing with neutrons is complicated because the environment where the tests are done also influences the results. Neutrons from the source act like billiard balls that can collide with walls many times before even reaching the detector. As the count rate of the detector may not follow the $1/r^2$ law, where r is the source-to-detector distance, the test facility needs to have large dimensions so that all surfaces are far enough away from the source and from the detector. This is not often the case.

Some detector manufacturing companies have their own (usually) nationally-accredited laboratories. However, seldom do they have strong metrologically traceable sources in them, and in these cases they have to rely on better-equipped laboratories.

Possible solutions and approaches

The testing facilities that the new security-driven developments demand for the performance evaluation, especially concerning radiation detectors, are currently been built by some EU Member States as well as by the IAEA and the JRC. The EU has recently contributed to making it possible for all EU Member States and their relevant stakeholders to have the necessary access to test facilities within the ITRAP+10 project. Thus, the JRC's ITU has opened two new laboratories exclusively dedicated to the static and dynamic testing of nuclear security detection equipment. The capabilities include testing new technologies with alternative ^{3}He neutron detectors.[50] This example, where all the manufacturers in Europe have participated with their equipment to the test campaign organised by the JRC, is a unique example of effective collaboration.

Simultaneously, as recommended by the EU CBRN Action plan adopted by the European Council in December 2009[51], the European Nuclear Security Training centre (EUSECTRA) has been established by the JRC in Karlsruhe to serve as a platform for knowledge transfer and for networking of experts. The facility offers a comprehensive training scheme for first responders,

[50] The tests, developed jointly with the US partners under the coordination of Domestic Nuclear Detection Office (DNDO) and with the collaboration of the International Atomic Energy Agency (IAEA), are mainly based on the ANSI and IEC standards. See http://itu.jrc.ec.europa.eu/fileadmin/EUSECTRA/ITRAP%2B10%20hand%20held%20lab.pdf and http://itu.jrc.ec.europa.eu/fileadmin/EUSECTRA/ITRAP%2B10developments_dynamic.pdf.

[51] Communication from the Commission to the European Parliament and the Council on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan, Brussels, 24.6.2009 COM(2009) 273 final: http://ec.europa.eu/home-affairs/summary/docs/com_2009_0273_en.pdf. See also: http://itu.jrc.ec.europa.eu/index.php?id=36&type=0&iEntryUID=246&iEntryPID=68 and http://europa.eu/rapid/press-release_IP-13-338_en.htm.

measurement expert support teams and nuclear forensic experts comprising practical and table-top exercises.

Thus, while there still are challenges and possible gaps within the field of RN testing in the EU, these challenges are well identified and the processes dealing with them are in place.

5 OPTIONS FOR ENHANCING EU CAPABILITIES

The Security Industrial Policy Action Plan Communication[52] sets forward a master plan to enhance the European security industry, highlighting especially the gap between the European and US industries as well as the upcoming challenges from the Asian industries. Identifying the fragmentation of the European security market as a key obstacle, the Communication's focus is on European-level standardisation and certification. Furthermore it takes up issues such as how to reduce the time from research to market.

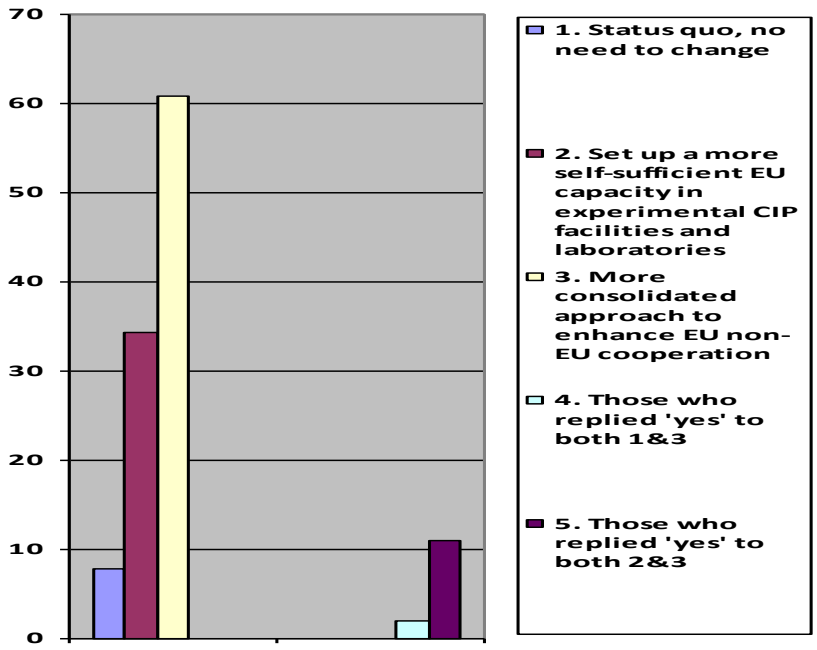
However, the Communication does not explicitly deal with the question of testing, nor is there any other European-level debate or plan on how to enhance the capabilities for testing security solutions from the current level, beyond normal national and company-level development plans, and some sectoral developments, e.g. in the RN field, as discussed in this paper. A more concerted approach is needed to enhance European CIP-related testing capabilities. This section considers the pros and cons of the different approaches that could be taken at EU level to enhance testing capabilities.

5.1 Alternative approaches

The ERNCIP survey presented to respondents three options which could form an approach to enhance the testing capabilities in the field of CIP security solutions. As Figure 5 shows, an overwhelming majority of respondents supported a more consolidated approach to enhance EU/non-EU cooperation. The approach to set up a more self-sufficient EU capacity in experimental CIP facilities and laboratories received support from almost a third of the responders, whereas the status quo option, i.e. do nothing, was supported only by a tenth of the respondents. This result clearly signals a demand for change. The results also show that there is some support to combine options 2 and 3, i.e. striving for EU self-sufficiency while at the same time enhance cooperation with non-EU actors.

[52] Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Security Industrial Policy. Action Plan for an innovative and competitive Security Industry Brussels, 26.7.2012. SWD(2012) 233 final. COM(2012) 417 final: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF.

Figure 6: Best way to go ahead (%, n= 65)



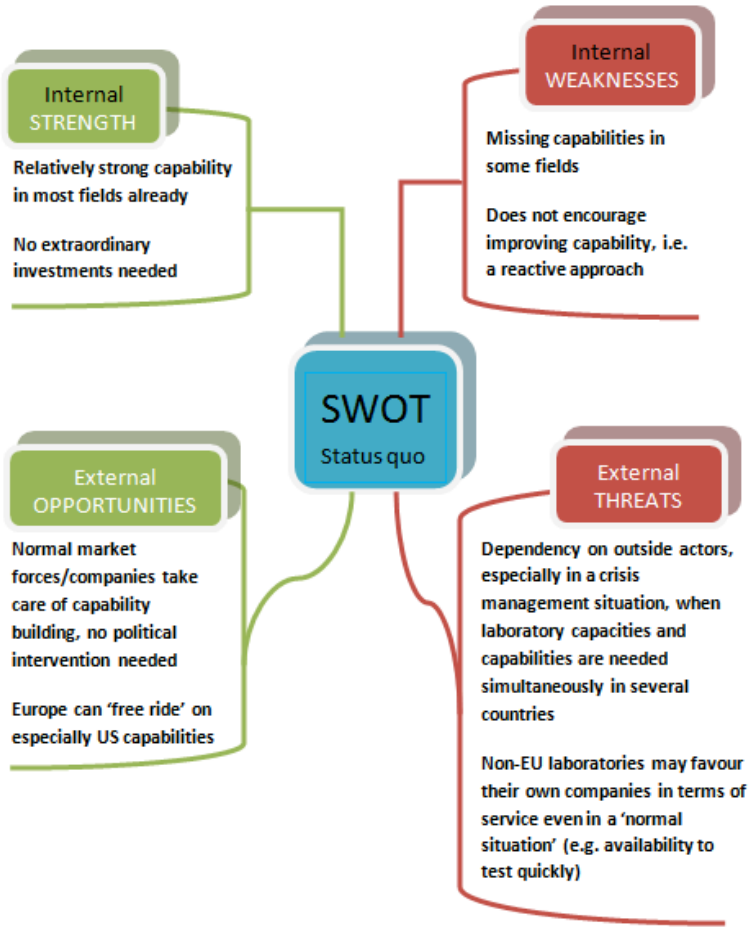
On the basis of these results, we have considered the four most plausible alternatives in some detail, using SWOT analyses, where the internal SWOT dimension refers to each approach's *own* strengths/merits or weaknesses/demerits, and the external SWOT dimension refers to possible contextual opportunities and threats that may affect the outcome of the respective approach. The four approaches are:

1) Maintain the status quo;
2) Set up a more self-sufficient EU test capability;
3) A more consolidated approach to cooperation with non-EU laboratories;
4) A combination of approaches 2) and 3).

5.2 'Status quo'

No evidence of plans or on-going debate concerning the level of European experimental and testing capabilities has been identified outside of ERNCIP, which implies no need exists for an EU-level programme to enhance the experimental and testing capabilities. However, making no change to the current situation received the lowest support among the ERNCIP survey respondents (less than 8 %), which indicates that stakeholders are dissatisfied with the current situation.

Figure 7: SWOT of 'Status quo' approach to testing capabilities in the EU



The positive sides of this option, as presented in Figure 7, are based on the argument that Europe already has several experimental facilities and laboratories for testing security solutions, and good capacity and capability in most fields. This report has shown that the current problem areas may be more due to the lack of harmonised regulatory frameworks than to lack of testing capability. This option assumes that normal market forces should and would meet any need for additional testing capabilities, and that the EU can continue to benefit from the current 'free riding' on the capabilities of other nations, especially on US experimental and testing facilities.

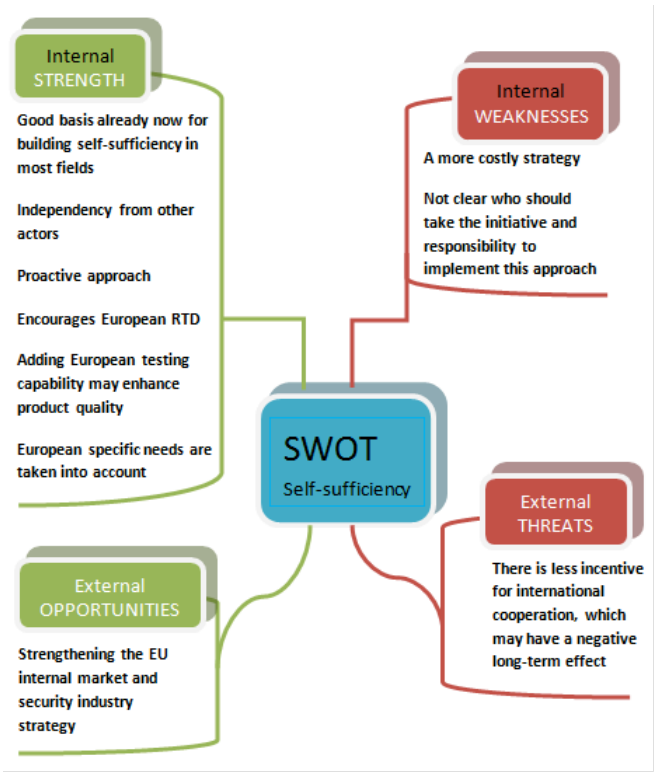
This passive approach has the disadvantage that it does not encourage further development of capability. The EU may lose the initiative in technology development, and it will not capitalise on all the potential within the EU. A system based on reliance on outside capabilities may also discriminate against some EU-based companies vis-à-vis non-EU companies, and does not support the European security industry, and associated RTD. Most notably, from the security

point of view, the status quo approach leaves Europe dependent on outside testing capabilities and capacities that might not be always available when needed.

5.3 'Self-sufficiency'

Greater self-sufficiency in the EU in the capabilities to test security solutions was supported by around 35% of respondents to the ERNCIP survey. The SWOT analysis of this option in Figure 8 below presents some clear benefits.

Figure 8: SWOT of building up EU 'Self-sufficiency' in testing capabilities



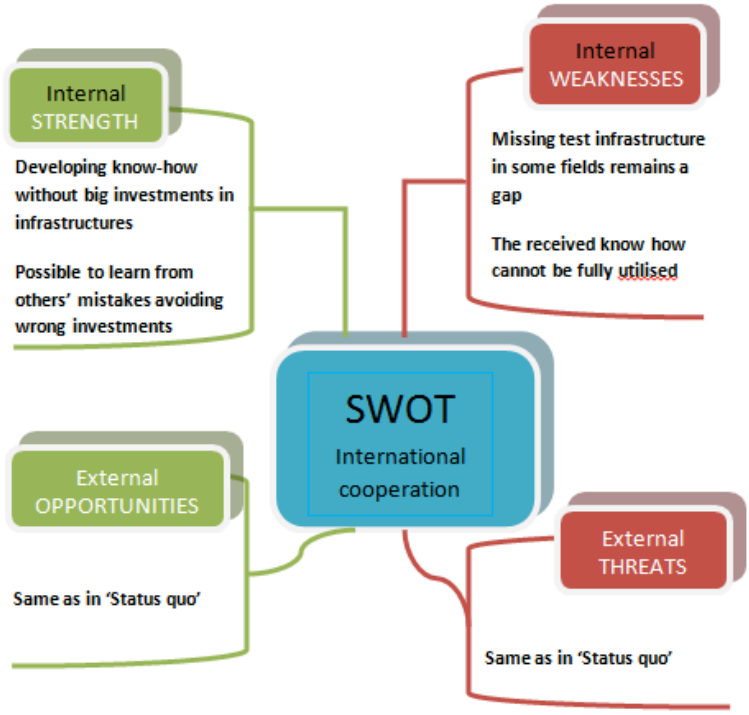
Most notably, it would make the EU less dependent on outside capabilities in fields that might become critical and difficult to access in future emergency situations. It would be a more proactive approach, which implies more RTD investments in the security industry, requiring an active EU policy to this effect. Another important benefit of a test capability independent from the US is that it could better take into account any specific European needs.

On the negative side, the approach will require increased investment and it is unclear where the responsibility to build up this self-sufficiency would best lie; with the EU, the Member States, the laboratories, or the security industry (companies)?

5.4 'International cooperation'

The third option to enhance the testing capabilities offered in the ERNCIP survey was more cooperation with non-EU experimental facilities and laboratories, which obtained most support (61%).

Figure 9: SWOT of enhancing 'International cooperation'

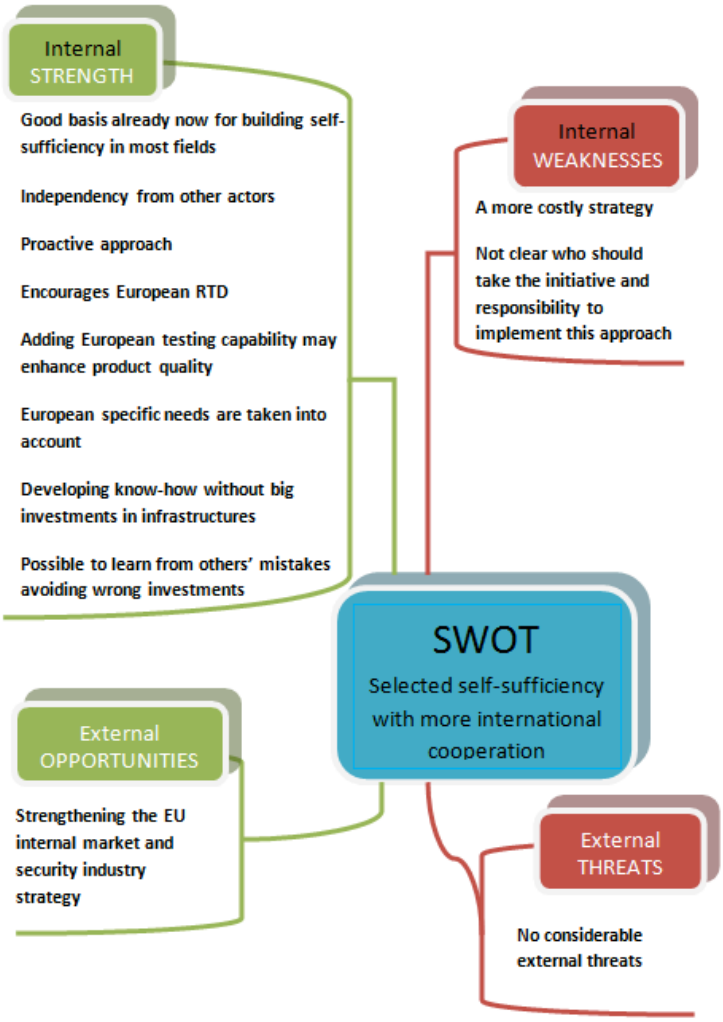


This option is similar to the 'Status quo' but it makes more use of international cooperation than is today the case. In a sense it enhances European testing capabilities but only in terms of know-how. Otherwise it bears the same pros and cons as the 'Status quo'.

5.5 Selected 'Self-sufficiency' with more 'International cooperation'

The fourth option is a combination of the two previous approaches: enhance Europe's own capabilities in some areas while at the same time making full use of the cooperation potential. On the basis of the ERNCIP survey, this approach would perhaps best satisfy the needs of most CIP stakeholders.

Figure 10: SWOT of selected 'Self-sufficiency' and enhanced 'International cooperation'



This option would combine the best parts of the previous two alternative approaches. In fact, this kind of approach has previously been proposed. Among others, the previously-mentioned 2004 *Research for a Secure Europe* report[53] notes that in many cases US options could meet also a number of Europe's needs, and that Europe's response should include not one but a variety of approaches, depending on the type of technologies. Emphasis for greater cooperation should be placed on security areas that require a particularly high degree of international cooperation. However, for the most critical security technologies, and also for technologies where requirements in Europe are different, Europe should consider an indigenous competitive capability, even if this involves duplication of US capabilities.

[53] *Research for a Secure Europe* (2004), op. cit.

5.6 Prioritisation methods for increasing self-sufficiency

How might the EU be able decide on the areas that would justify self-sufficient capabilities? As illustrated in Table 4, a starting point could be to look at two factors: the *criticality* of the missing capability for security testing, and the *costs* involved.

The resulting matrix could then be used to produce priorities for EU actions. In this *theoretical* example, five priorities are suggested, ranging from 1 (High) to 5 (Low), but the complexity and categorisation can be modified to suit the requirements of the stakeholders. If a missing specific testing capability has a high criticality to Europe's security, and at the same time would involve low costs, this would fall into the top priority (Priority 1), as a potential "quick win". Similarly, a very costly investment in a capability which has a low criticality should be prioritized lowly (Priority 5). Clearly, the decision-making for EU-level investments will need to be based on well-informed analysis.

Table 4: A theoretical method of prioritisation

Capability lacks	**Costs and other resources/time needed to build self-sufficiency**			
Criticality of the missing capability/ Specific EU needs		Low	Medium	High
	High	Priority 1 ("quick wins")	Priority 2	Priority 3
	Medium	Priority 1 ("quick wins")	Priority 3	Priority 4
	Low	Priority 2	Priority 4	Priority 5

6 CONCLUSIONS AND RECOMMENDATIONS

This paper provides tentative findings about the gaps in European experimental and test capabilities for CIP-related security solutions. This section summarises the key conclusions and makes recommendations, for a possible way forward.

6.1 Conclusions on the current situation

EU lacks some experimental and test capabilities. ERNCIP stakeholders cooperate with non-EU experimental facilities and test laboratories not only in order to receive certification for access to the respective non-EU countries' markets, but also because they do not find necessary test capabilities in the EU. From the ERNCIP survey and from the information received from ERNCIP Thematic Groups, it is obvious that there are some gaps – though not in all fields - in the EU both in terms of expertise and know-how as well as test infrastructure and equipment.

No detailed picture is available about the capabilities and gaps. There is no single actor who has a holistic, cross-sector picture of the EU experimental and test capabilities for CIP-related security solutions. Even within separate sectors, the available data turns out to be fragmented and superficial; the laboratories are usually aware of only their own capabilities, and if the capabilities are hard to list, it is even more difficult to confirm the gaps.

Test capabilities are related to standards. The notion of EU experimental and testing capabilities for CIP-related security solutions is closely connected to the issue of common international or European standards, common test methodologies and mutually recognized certification schemes. In the absence of these, it is difficult to assess what are the requirements for a test facility, and where exactly the serious gaps are in the EU in this context.

Multiple ways to enhance capabilities. The examples discussed in this paper show that there are multiple ways to fill in capability gaps: sometimes capability enhancement is taken care by market forces (companies build up their laboratories); EU-funded projects have introduced innovative resource pooling practices; Member States have upgraded their national capabilities by direct funding; Member States together with the EU have agreed upon capability building, e.g. in the context of the JRC; public-private partnerships (PPP) have been used.

No overall European master plan to enhance test capabilities. There is however no horizontal, cross-cutting European master plan on how to identify and fill in the gaps in CIP-related testing capabilities. Within some sectors, such as radiological and nuclear risks, there are examples of how the European experimental and test capabilities have been enhanced and the identified gaps

filled in. The experience shows that to achieve an effective and tangible solution, a gap, and the respective need to fill it, have to be articulated in an EU policy document (cf. EU CBRN Action Plan), with a clear mandate, implementation structure and necessary funding.

6.2 Recommended way forward

6.2.1 High-level approach

For the way forward, this report recommends adoption by the EU of an overarching policy to improve CIP by enhancing EU CIP-related security solution testing capabilities, based on an approach which combines selectively building up test capabilities in the EU, while enhancing cooperation with non-EU experimental facilities and test laboratories. As the primary driver of this policy will be the improvement of CIP in the EU, this policy should come under the umbrella of the EPCIP programme, being managed by DG HOME

Under this high-level policy, sector/thematic-level activities will enable a focussed approach towards European testing capability building, coordinated with the on-going process of creating, harmonising and validating European security standards. There are several on-going cross-cutting efforts (such as CEN/CENELEC, ERNCIP etc.) as well as sectoral efforts (such as ECAC, ENISA, individual FP7 projects) where issues such as developing a harmonized European regulatory framework, standardization, common test methodologies and mutually-recognized European certification schemes are already being discussed and developed.

6.2.2 Road Map of next steps

The issue of testing capability building should be added to the issues to be dealt with in more detail within the potential future phase of ERNCIP, so that capability building can be better coordinated with the on-going processes of creating and harmonising standards. While ERNCIP can act as a catalyst and provide the framework for these processes, the relevant stakeholders within the European Commission will need to identify the most suitable funding framework.

The way forward should include the following steps:

1. Develop further the issues discussed in this paper by organizing an ERNCIP workshop on experimental and test capabilities in the EU with regard to CIP-related security solutions. This could be organised within the current ERNCIP programme in 2014. The aim of this workshop should be to reach a common general agreement among the key stakeholders about where capability building is most needed.

2. Where the need to **enhance specific CIP-related experimental and testing capabilities in the EU is identified**, multi-stakeholder sectoral thematic working groups should be established within ERNCIP, or the issue added to the mandate of an existing ERNCIP Thematic Group already dealing with other related issues. An appropriate timeline for addressing this issue would be around a year.

3. These working groups should identify, list and evaluate the concrete know-how and infrastructure gaps and development challenges in EU-based experimental and testing capabilities within the respective sector, based on validated information. Each working group should prepare a sector capability and gap evaluation.

4. This evaluation should include prioritisation; cost-benefit calculations of development needs, based on criticality, costs and other factors, should be made.

5. Furthermore, in the evaluation, the working group should analyse the different solutions available to fill in the gaps. The alternatives include EU-led and EU-funded approaches (e.g. JRC, FP7 projects), Member State–based approaches, market-based approaches (companies), combinations of the former (PPP), and other possible solutions.

6. Finally, detailed ERNCIP recommendations, using the ERNCIP Expert Group (which represents the Member States' CIP authorities) as an additional advisory body, should be made to the relevant policy, funding and implementation bodies.

7. Ideally, these ERNCIP recommendations will be considered by the respective EU policy areas, with concrete policy conclusions articulated in relevant EU policy documents.

8. Where a **the need for more focussed approach towards international cooperation is identified** such cooperation, particularly in RTD and training, should be enhanced with more coordinated European-third party programmes. The potential future ERNCIP (2015-2020) could work as a tool or platform also in this respect, and a framework of how the international partners could participate in ERNCIP Thematic Group meetings, as guest members, should be prepared.

European Commission
EUR 26229 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **European CIP-related Testing Capabilities: Gaps and Challenges**

Authors: Christer Pursiainen, Peter Gattinesi

Luxembourg: Publications Office of the European Union

2013 – 55 pp. – 21.0 x 29.7 cm

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

ISBN 978-92-79-33760-4

doi:10.2788/34627

Abstract

One of ERNCIP's goals is to identify gaps in European CIP-related experimental and testing capabilities, and to set up a wider debate on how to deal with these gaps. This report draws an indicative picture about the known state of European CIP-related test capabilities. The analysis is primarily based on an ERNCIP online questionnaire on the issue circulated at the end of 2012, which was completed by 65 respondents representing different types of ERNCIP stakeholders. The ERNCIP Thematic Groups have also provided information about their respective capabilities and perceived gaps in their sectors. This report aims to provoke further debate among the ERNCIP stakeholder communities.

LB-NA-26229-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

ISBN 978-92-79-33760-4

9 789279 337604