SUPPORTED UNDER:

SEVENTH FRAMEWORK PROGRAMME

FIRE

Gateway to trustworthy ICT innovations in Europe

PROJECT FULL TITLE: **F**acilitate **I**ndustry and **R**esearch in **E**urope

GRANT AGREEMENT N. 318762

DELIVERABLE D2.2

Identification of Trans-Cluster Research Complementarities and Gaps

Due Date : 28 02 2013
Main Author : C Pickering, N Adams, R Chisnall
Contributors: ADS, AMETIC, CYBERNETICA, IFIS, LSEC, NSMC
Dissemination : PU

Document Control Sheet

Project Number	318762	
Project Acronym	FIRE	
Work-package:	2	
Last Version:	V2.0	
Issue Dates:		
Version 1. D2.2 v1.0	28/02/13	
Version 2. D2.2 v1.1	18/03/13	*Key messages added*
Version 3. D2.2 v1.2	18/03/13	*Minor revisions*
Version 4. D2.2 v1.3	20/03/13	*Minor revisions*
Version 5. D2.2 V2.0	09/04/13	*Revision marks removed*

Classification

This report is:

Draft	
Final	X
Confidential	
Restricted	
Public	X

Partners Owning	ADS
Main Editor	ADS/ LSEC

Partners Contributed	ADS, AMETIC, CYBERNETICA, IFIS, LSEC, NSMC

Table of Contents

1 EXECUTIVE SUMMARY

This public report represents Deliverable D2.2 from Task 2.3 of the FIRE project.

The ultimate aim of the FIRE project is to stimulate Trustworthy ICT research and industry cooperation to underpin the EU competitive position and produce a pan-cluster research agenda, taking account of end-user and IT security solution providers' needs and the strengths and weaknesses of different Member States, with recommendations for its implementation.

To identify initial complementarities and gaps between the regions, the FIRE project partners have carried out an initial analysis for their countries/ regions, aimed at identifying the key issues that each region needs to address to enhance its IT security capability and competitiveness, and the resulting IT security research priorities. The results were presented at a FIRE strategy workshop on 14th – 15th February, and an initial analysis of the results was then performed. The aim of this report is to provide an overview of the initial results and analysis.

The following key messages emerged from the workshop:

Physical control systems (SCADA) and the Internet of Things

- Recognition of IT Security issues across most partners concerning SCADA systems, particularly legacy systems, with variable responses across Member States.

Certification (Standards) for individuals

- Certifications for professionals (and training) vary across the partner countries: national schemes dominate in some Member States and can impede the free movement of services within the EU as a whole.

Strategy and funding

- Absence of a national ICT Security Policy/Strategy in Belgium, Czech Republic and Spain, contrasting strongly with mature strategies in Estonia, Germany and the UK.

Skill shortage/ training/ education

- Availability of skilled staff is very variable across Member States. In the UK the IT Security skills gap is estimated to take up to 20 years to address.

Security Economics

- There are strong concerns in each Member State about the capability of companies to quantify IT Security risks to underpin sound business cases for addressing them.

SMEs

- All Member States had concerns over the resilience of the SME supply chain. Estonia has developed a compulsory 3-level IT baseline security system, ISKE 2003, with a minimum baseline level well suited to SMEs. Standards in use in other partner countries, e.g. ISO27001, are considered too resource intensive for SMEs.

In addition the following application areas were identified as being of concern across the partner regions:

- CIIP (Critical International Infrastructure Protection)
- Smart Meters/ Smart Grids
- I-Voting (Estonia only at present)
- Cloud and mobile based services (and forensics)

Further analysis of the information was carried out after the workshop to identify potential complementarities and gaps between the regions that could form the basis of joint policy and research cooperation. Areas of joint strength in two or more regions for which cooperation could give mutual benefit, and areas where some regions had strengths other regions could benefit from, were identified. These opportunities for joint work by the FIRE partner countries will be investigated in more detail in the next stage of the project.

Examples of technical (research) challenges to address have been identified but they have not yet been prioritised to take account of IT security provider and end user needs. This will take place in the next stage of the project and further development of the joint research agenda will be the focus of the next FIRE Strategy Workshop.

2 INTRODUCTION AND PURPOSE OF THE REPORT

The aim of this report is to provide an overview of the initial results and analysis of the information collected by the FIRE partners on the IT security research activities and capabilities in their countries, the environment in which they operate, and the local needs that drive them. The data collection is based on the methodology produced in Deliverable D2.1[1].

This is a public report representing Deliverable D2.2 from Task 2.3 of the FIRE project. The detailed national findings are not included as they will be revised and completed over the next phase of the project. The output of this task will be combined with information on end-user and IT security industry needs from Work Package 3, together with information from other Work Packages, to allow the consortium to identify areas for pan-cluster cooperation and to develop the pan-cluster research agenda.

[1] Deliverable 2.1 – FIRE Research and Innovation Analysis Methodology: 30 Nov 2012

3 CONTEXT

The ultimate aim of the FIRE project is to stimulate Trustworthy ICT research and industry cooperation to underpin the EU competitive position and produce a pan-cluster research agenda, taking account of end-user and IT security solution providers' needs and the strengths and weaknesses of different Member States, with recommendations for its implementation.

The first phase of this activity requires development of an understanding of the relative strengths and weaknesses of the research activities in the partner regions, in order to identify complementarities and significant gaps, and hence areas where trans-national cooperation may be beneficial. This will also highlight areas of common concern that are not being addressed by any of the partner regions and could form the basis of recommendations to national and EU policy makers.

In a second, parallel phase, end-user and IT security industry needs will be identified through a series of meetings and discussions in the partner regions organised via a series of Industry and Commercial Networks (ICNs) in Finance, Health, Energy, Mobile Communications and Government.

This report, based on the tasks in Work Package 2 to collect and analyse data and supporting information on the current situation in the partner regions, provides an overview of the initial findings of the first phase activity outlined above.

4 METHODOLOGY FOR DATA COLLECTION (FRAMEWORK) AND ANALYSIS

Deliverable D2.1 described a framework for collection and analysis of regional capabilities and activities[1]. A research agenda is being produced for each region by the partners covering the elements as described below with associated questions to capture the required information. Templates for data collection based on these headings were provided to the partners by the Work Package 2 leader (ADS). This was to facilitate data collection in a common format for analysis, and also to provide a common structure for partner presentations at the Strategy Workshop to make it easier to identify initial areas of complementarity and common concern. Examples of stakeholders being used as data sources in the UK were also provided to the partners to guide their data collection activities.

This framework will also be used to develop the joint pan-Cluster research agenda and action plan. The regional information will be used in combination with other supplementary information on Industry needs (Work Package 3), national RTD activities (Work Package 4), innovation pull-through best practice (Work Package 5) and analysis of how to address societal concerns (Work Package 6) to support pan-Cluster strategy development.

In Year 1 (for the work leading to a draft joint research agenda in Month 12) the partners are focusing on collecting data for their countries, while in Year 2 they will also consider activities in neighbouring countries when updating their view on regional priorities, for the production of the final joint research agenda in Month 24.

The research agenda elements being considered are:

A) VISION FOR THE FUTURE

B) CURRENT SITUATION

1. ENVIRONMENT (CONTEXT)

2. IT SECURITY CUSTOMERS

3. IT SECURITY INDUSTRY CAPABILITY

4. IT SECURITY RESEARCH CAPABILITY

5. NATIONAL INITIATIVES AND PROGRAMMES

6. POLICY AND REGULATORY ISSUES

7. STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS IN IT SECURITY

8. COMPETITION AND COMPETITIVE ADVANTAGE

C) RESEARCH AGENDA AND ACTION PLAN

The data collection process was undertaken through a variety of stakeholder discussions and desk research as appropriate in the partner clusters. As an example, the following methods were used in the UK.

Data sources:

- Academic Centres of Excellence (ACE) in Cyber Security Research presentations at Inaugural Conference, Cheltenham
- UK Cyber Security Strategy
- Research Council data on projects and research institutions
- UK Government publications on R&D and training programmes

Interviews and visits:

- Government Communications Headquarters (GCHQ)
- Centre for the Protection of National Infrastructure (CPNI)
- ADS/ Cyber Protection and Assurance Group
- UK Government Department of Business Innovation & Skills (BIS)
- UK Digital Knowledge Transfer Network (KTN)
- Engineering & Physical Sciences Research Council (EPSRC)
- Selected ACE universities and large industrial companies
- Finance Industrial and Commercial Network meeting, London
- Malvern Cyber Security Cluster

Conference information and desk research.

5 INDIVIDUAL COUNTRY RESULTS

To identify initial complementarities and gaps between the regions the FIRE project partners carried out an initial analysis for their countries, aimed at identifying the key issues that each region needs to address to enhance its IT security capability and competitiveness, and the resulting IT security research priorities:

- ADS: UK
- AMETIC: Spain
- CYBER: Estonia (also considering Scandinavia and the Baltic states)
- IFIS: Germany
- LSEC: Belgium
- NSMC: Czech Republic

These results were presented at the FIRE Strategy Workshop on 14th – 15th February 2013. These results and the supporting information provided have been analysed to identify complementarities and gaps between the partner countries in IT security activities, and the implications for IT security research. The next step for partners will be to prepare a research agenda and roadmap for their countries, starting from the SWOT and competitive advantage analysis and inputs from other work packages.

6 ANALYSIS

During day one of the joint cluster workshop on 14 February 2013 key national issues were identified by partners. A review of the findings on day two of the workshop identified the following key issues that were important to all the regions:

- Physical control systems (SCADA)
- Certification (Standards)
- State Legislation (and voluntary measures)
- Skill shortage/ training/ education
- Size of market (to justify investment in new solutions)
- Business Case
- SMEs
- Supply chain reliance on the US
- Secrecy

These top level issues of common concern were then developed further and broken down into key components, generating the following provisional taxonomy:

1. ***Physical control systems (SCADA)***
   1.1. M2M, Internet of things
   1.2. Smart Grids / Smart metering
   1.3. CII / CNI
2. ***Certification (Standards)***
   2.1. Certification for professionals
   2.2. Trans-border recognition of certification schemes
   2.3. Presence of national or international standards recognised for organisations
3. ***State Legislation (and voluntary measures)***
   3.1. Legislation used as a driver
   3.2. Trans-national applicability
   3.3. Government provides a lead
4. ***Strategy and funding***
   4.1. National Cyber Security Policy
   4.2. Financial support for R&D programmes
5. ***Skill shortage/ training/ education***
   5.1. Shortage of staff
   5.2. Existence of good in-country training programmes
6. ***Capabilities and Market***
   6.1. Academic strengths (to do research)
   6.2. Industrial strengths (to supply solutions)
   6.3. Presence of EU suppliers in the home market
7. ***Business Case***
   7.1. General awareness
   7.2. Justification is understood
   7.3. Availability of good case studies
   7.4. Understanding of the market
   7.5. Justification is used and investment made
8. ***SMEs***
   8.1. Perception of SME vulnerability
   8.2. Appropriate standards exist/used for businesses of different sizes (ISO 27000 is too complex for SMEs)

Each partner was asked to score their national perception of the issues above using a quantified scale. Examples of variations between partner countries highlighted by these results and the analysis by the FIRE partners are described in the following table:

TABLE 1 – VARIATIONS IN IT SECURITY APPROACHES AND CONCERNS BETWEEN FIRE PARTNER COUNTRIES

No.	Issue	Variations in IT Security approaches and concerns between partner countries
1.	Physical control systems (SCADA)	Strong IT Security concerns across most partners about SCADA systems, particularly Legacy systems, although Estonia with its strong security management regulations and security experience appears better prepared than some other countries.
2.	Certification (Standards)	Certifications for professionals (and training) vary across the partner countries: there are no national certifications for professionals and a lack of IT Security training in Spain, while there are several certification systems used in the UK and Germany with associated training programmes.
3.	State Legislation (and voluntary measures)	Czech Republic lacks legal framework for securing cyber space and Belgium has limited regulatory programmes, while other partner countries have well developed frameworks in place.
4.	Strategy and funding	Absence of a national ICT Security Policy/ Strategy in Belgium, Czech Republic and Spain, contrasting strongly with mature strategies in Estonia, Germany and the UK.
5.	Skill shortage/ training/ education	The UK has an IT Security skills gap that it could take up to 20 years to address (at all levels of education)[2], while Belgium is better placed to meet its demand from local research organisations and companies.
6.	Capabilities and Market (Supply chain reliance on the US)	Non-EU suppliers of IT Security products have a dominant position in most partner countries but EU (and national) suppliers play a greater role in the German market.
7.	Business Case	There are strong concerns in the partner countries about the capability of companies to recognise IT Security risks and produce sound business cases for the investment needed to address them. There is perceived to be a better understanding and approach in equivalent

[2] NAO Report: The UK cyber security strategy: Landscape review - dated 12th February 2012.

		businesses in Germany: the reasons for this require further analysis.
8.	SMEs	Estonia has developed a compulsory 3-level IT baseline security system, ISKE 2003, with a minimum baseline level well suited to SMEs. Standards in use in other partner countries, e.g. ISO27001, are too resource intensive for SMEs.

The following application areas were initially identified as being of concern across the partner regions:

- CIIP (Critical International Infrastructure Protection)
- Smart Meters/ Smart Grids
- I-Voting (Estonia only at present)
- Cloud and mobile based services (and forensics)

Further analysis of the regional data was then carried out to identify potential complementarities and gaps between the regions that could form the basis of joint policy and research cooperation. Major differences across countries were explored in more detail to identify areas where cooperation might be of benefit. Areas of joint strength in two or more regions where cooperation could give mutual benefit were identified, and areas where some regions had strengths other regions could benefit from. These opportunities for which joint work by the FIRE partners/ partner countries might be of mutual benefit will be investigated in more detail in the next stage of the project.

7 RESULTS AND NEXT STEPS

The next step is for FIRE partners to develop a research agenda and roadmap for their countries. Examples of technical (research) challenges to address identified across the partner regions so far are:

- Situational awareness (and its impact on business)
- Formal methods for secure large systems
- Secure multi-party computing, computing on encrypted data
- How to deal with unknown threats by incorporating resilience at all levels (processes, technologies, people)
- Secure identity management and strong authentification - models based on passwords are archaic: biometrics, identity management, super-identities, security protection, security of RBAC policies, multifactor authentification for cloud services etc
- Cyber-physical systems, security by design, web privacy, trust & provenance, Privacy enhancing technologies
- Anonymisation of linked datasets, internet & web law, extremist ideas online
- Cyber risk management, application to financial markets and banking, network security, eCash
- SCADA and related (industrial automation), automotive systems security, smart grid & meters
- Cryptography including fully homomorphic encryption and emerging technologies, e.g. lattice-based cryptography
- Embedded security (built in security is becoming a USP), Near Field Communications e.g. for Health and Internet of Things, electromagnetic security, circuit watermarking.

Further technical challenges will be identified and prioritised, together with the initial list mentioned in the previous section, to take account of IT security provider and end user needs identified by the Industry and Commercial Networks. Following development of the individual research agendas for the partner countries a joint pan-cluster research agenda will be developed. This will identify options for cooperative research projects, which could be supported by national and EC funding bodies.

The FIRE partners will also explore the gaps and synergies between the partner countries in more detail, starting by reviewing initial opportunities for cooperation suggested in the initial analysis to date, as follows:

PHYSICAL CONTROL SYSTEMS (SCADA)

1) FIRE partners to investigate whether there is scope for joint research projects to address common SCADA vulnerabilities e.g. in Energy.

CERTIFICATION (STANDARDS)

2) FIRE partners to review certifications for professionals (and training) in use across partner countries and identify best practice that can be used by FIRE partners and their networks.

3) LSEC to coordinate review of IT security standards in partner countries to see where common standards would have the most impact, and make recommendations for the EC.

STATE LEGISLATION (AND VOLUNTARY MEASURES)

4) FIRE partners to review whether there are any actions the project can take to help address differences in EU legal frameworks that restrict the EU-wide market size for IT security products.

SKILL SHORTAGE/ TRAINING/ EDUCATION

5) FIRE partners to review how education and awareness raising is done across partner countries and identify best practice examples that can be used by FIRE partners and their networks.

CAPABILITIES AND MARKET

6) ADS and LSEC to explore options for developing joint EU solutions for the Finance Industry that exploit synergies between FIRE partners and their networks.

7) ADS and NSMC to explore options for collaboration between UK and Czech members in complementary areas.

8) ADS, IFIS, LSEC and CYBER to investigate scope for cooperation in cryptography between researchers and EU companies.

9) FIRE partners to investigate scope for joint research projects that can build on Estonian experience in ICT implementation to help develop new EU security products.

10) FIRE partners to investigate scope for joint research projects that can build on German experience in smart grids and smart meters to help develop new EU IT security products.

11) ADS and IFIS to investigate whether UK Research Councils and German research funding bodies are in contact and whether bilateral collaboration might be considered.

12) FIRE partners to review whether forensics in law enforcement is an area where joint EU funding support of R&D and implementation would benefit the EU.

13) FIRE partners to review how SME innovations are supported across partner countries and identify best practice examples that can be used by FIRE partners and their networks.

14) FIRE partners to review industry-research cooperation models across partner countries and identify best practice examples that can be used by FIRE partners and their networks.

BUSINESS CASE

15) FIRE partners to investigate what market data is available to support investment in developing privacy and trust related security products.

16) FIRE partners to compile case studies of threats, attacks and potential losses that can be promulgated to raise awareness in FIRE partner networks, looking at examples

currently available.

17) FIRE partners to investigate what sources of data exist on the IT security market size and nature that could support investment cases in partner countries, building on previous work.

18) FIRE partners to identify if work on the cost of cyber-crime to their countries has been carried out, compare this to UK and any EU-wide figures, and consider what a better methodology to calculate this cost might be.

19) FIRE partners to investigate whether there is best practice in development of business cases in Germany that could be applied in other partner countries.

THREAT

20) FIRE partners to identify options for providing monitoring and traffic analysis capabilities for network traffic, and make recommendations to MS/ EC.

21) FIRE partners to investigate opportunities to collaborate with the new CIP-ICT PSP-2012-6 ACDC (Advanced Cyber Defence Centre) pilot project that addresses the identification, measurement, and analysis of botnets as well as prevention, detection, mitigation, recovery, and evaluation of their impact.

SMEs

22) FIRE partners to review Estonian ISKE system to see if it could be employed in partner countries for the benefit of SMEs.

8 CONCLUSIONS

The FIRE strategy workshop on 14th – 15th February identified the following key issues that were important to all the regions:

- Physical control systems (SCADA)
- Certification (Standards)
- State Legislation (and voluntary measures)
- Skill shortage/ training/ education
- Size of market (to justify investment in new solutions)
- Business Case
- SMEs
- Supply chain reliance on the US
- Secrecy

In addition the following application areas were identified initially as being of concern across the partner regions:

- CIIP (Critical International Infrastructure Protection)
- Smart Meters/ Smart Grids
- I-Voting (Estonia only at present)
- Cloud and mobile based services (and forensics)

Further analysis of the regional data was carried out after the workshop to identify potential complementarities and gaps between the regions that could form the basis of joint policy and research cooperation. Areas of joint strength in two or more regions where cooperation could give mutual benefit, and areas where some regions had strengths other regions could benefit from were identified. These opportunities for which joint work by the FIRE partners/ partner countries might be of mutual benefit will be investigated in more detail in the next stage of the project.

Examples of technical (research) challenges have been identified but they have not yet been prioritised to take account of IT security provider and end user needs. This will take place in the next stage of the project and further development of the joint research agenda will be the focus of the next FIRE Strategy Workshop.