Metadata of the chapter that will be visualized in SpringerLink

Book Title	Cyber Security and Privacy	
Series Title	7899	
Chapter Title	Coordination of Trust and Security Project Clustering	
Copyright Year	2013	
Copyright HolderName	Springer-Verlag Berlin Heidelberg	
Corresponding Author	Family Name	**Clarke**
	Particle	
	Given Name	**Jim**
	Suffix	
	Division	
	Organization	Waterford Institute of Technology—Telecommunications Software and Systems Group
	Address	Waterford, Ireland
	Email	jclarke@tssg.org
Author	Family Name	**Malone**
	Particle	
	Given Name	**Paul**
	Suffix	
	Division	
	Organization	Waterford Institute of Technology—Telecommunications Software and Systems Group
	Address	Waterford, Ireland
	Email	pmalone@tssg.org
Author	Family Name	**Bodeau-Pean**
	Particle	
	Given Name	**Catherine**
	Suffix	
	Division	
	Organization	ONYAX-CBPO
	Address	Paris, France
	Email	catherine.bodeau-pean@wanadoo.fr

Abstract	The DG Connect Unit H4 Coordination and Support Actions and Networks of Excellence took part in two conference sessions during the Cyber Security and Privacy EU Forum (CSP 2013) to collectively address their roles, and, in particular, how they might work together within a Project Cluster framework to the advantage of the research and innovation projects and to the programme as a whole, and particularly in the context of significant recent EU initiatives concerning Cyber Security Policy and a Network Information Security Platform. The morning session examined goals and timescales of the projects; the afternoon session looked in further detail at options and possibilities for the structure and modus operandi for a project cluster, ways forward towards a NIS Platform, and extending participation, influence, and effect to projects outside the immediate ICT trust and security community.

Keywords (separated by '-')	Cyber security policy - Trust - Privacy - Information security - Coordination - Project clusters

Coordination of Trust and Security Project Clustering

Jim Clarke[1(✉)], Paul Malone[1], and Catherine Bodeau-Pean[2]

[1]Waterford Institute of Technology—Telecommunications Software and Systems Group, Waterford, Ireland
{jclarke, pmalone}@tssg.org
[2]ONYAX-CBPO, Paris, France
catherine.bodeau-pean@wanadoo.fr

Abstract. The DG Connect Unit H4 Coordination and Support Actions and Networks of Excellence took part in two conference sessions during the Cyber Security and Privacy EU Forum (CSP 2013) to collectively address their roles, and, in particular, how they might work together within a Project Cluster framework to the advantage of the research and innovation projects and to the programme as a whole, and particularly in the context of significant recent EU initiatives concerning Cyber Security Policy and a Network Information Security Platform. The morning session examined goals and timescales of the projects; the afternoon session looked in further detail at options and possibilities for the structure and modus operandi for a project cluster, ways forward towards a NIS Platform, and extending participation, influence, and effect to projects outside the immediate ICT trust and security community.

Keywords: Cyber security policy · Trust · Privacy · Information security · Coordination · Project clusters

1 Introduction

In response to foreseen needs for the security of the digital infrastructure and information that is so vital to all aspects of the lives and livelihoods of its citizens, there is significant action by the EU, with emphasis on a Cyber Security Policy and directive [1], and related initiatives including the establishment of a Network Information Security (NIS) Platform [2]. AQ1

The Trust and Security (T&S) Coordination Action (CA) SecCord – *Security and Trust Coordination and Enhanced Collaboration*)[1] – is responsible for managing the annual CSP Conference in line with the formal objectives and commitments in its Description of Work,[2] and for running the two conference sessions –*Track* 14– reported here.

[1] http://www.seccord.eu/
[2] "Description of Work" forms Annex 1 of the Grant Agreement of a FP project.

M. Felici (Ed.): CSP EU FORUM 2013, CCIS 182, pp. 1–13, 2013.
DOI: 10.1007/978-3-642-41205-9_12,

The purpose of the Track 14 workshop was to look at the current *Coordination and Support Actions* (CSAs) and *Networks of Excellence* (NoEs) of DG Connect Unit H4 – Trust and Security, and, in particular, to explore how they can work together for maximum benefit to the research and innovation projects and to the programme as a whole. This has two linked components: how the CSAs and NoEs can work in concert, and to what ends; and how the Trust and Security research and innovation projects can collaborate and support each other through forming project clusters.

This paper provides an overview of the workshop, and examines its recommendations and goals for future action.

Project Clustering. The concept of bringing projects together into clusters goes back to the early days of the Framework Programme – known then as Concertation – with the objective of projects achieving more together collectively or in focussed groups rather than as individual entities. A cluster is drawn from projects with shared interests; it comes together to look at common problems and issues, provide mutual benefit and insights, reduce overlap, and help leverage of results and outcomes. Clustering of T&S projects had (re)started already with the recent EFFECTS+ CA,[3] and with specific interest groups such as PRIMCLUSTER, the in-built clusters of the NoEs, and the Working Groups of earlier projects. The objective of SecCord is to further develop the clustering process and its effectiveness, and, in so doing, further the goals of the above Cybersecurity policy and NIS initiatives.

At a minimum, a project cluster should provide for a recognizable identity, a strategic roadmap for research, a repository for results, and channels for dissemination. The clusters themselves should be further brought together to provide a coordinated set of results and outputs that contribute to the EU cyber security policy and strategy. This might be in the form of a high-level Network Information Security Cluster cooperation mechanism, established at European Union level, to allow for information exchange and could form an integral component of the proposed NIS Platform, whose main purpose is to assist with implementing the measures set out in the NIS Directive, e.g. to simplify incident reporting, ensure its convergent and harmonised application across the EU, and provide input to the secure ICT R&I agenda [3].

Structure of This Paper. After this introduction, Sect. 2 outlines the current position, with some of the obstacles to successful clustering and possible ameliorations, with some areas of clustering activity to be explored; Sect. 3 gives a brief account of the workshop itself; Sect. 4 discusses the findings and proposals by the workshop; and Sect. 5 gives our conclusions and principle recommended actions.

2 Current Position

A fundamental problem for participation in clustering has sometimes been a reluctance of projects to allocate resources that may prejudice the achievement of their formal objectives of the Description of Work (DOW); a way forward may be to earmark certain

[3] http://www.effectsplus.eu/

resources in the Grant Agreements of the projects, or to allocate funds to the clustering process to facilitate participation by projects. This concept should be investigated, both for current running projects and new projects currently in negotiations.

Three areas of clustering are identified:

1. Trust and Security Project Clusters as currently envisaged in the SecCord Description of Work, building on the earlier clustering activities of EFFECT-S + and developing the clusters to open up to other relevant domains, and, in particular, legal, social, economics, and health. SecCord already has the task to examine further mapping and alignment to achieve these extended goals. Other objectives are: to build on the topics where there are European strengths; to build up in areas seen to offer future opportunities, avoiding the waste of gaps and overlaps, and to jointly provide significant leverage and benefits.
2. Networking and Coordination Cluster for Trust and Security (CSAs and NoEs): the cluster management or coordination of this is also envisaged as a SecCord responsibility. The CSAs should collaborate amongst themselves to actively support the clustering activities. A similar model should be developed for bringing the R&I and NoE projects together and integrating activities and results, and also to add value, possibly using a similar structure to the earlier cooperation of the Future Internet Support Actions (see FISA[4]).
3. At the time of the workshop, the NIS Cluster was yet to be defined in terms of its structure and relationships, but is seen as a super-cluster that gathers, coordinates, and delivers material specifically for the NIS Platform. The success of the NIS Platform will call not only for strong moral support from European industry and commerce, but also for their active contribution and participation in the instruments of the platform. The way to tie-in and to incentivise participation of these communities effectively without overlaps is of utmost importance to the success and impact of clusters.

The first of these is already operational: the CSP conference, of which these two sessions were a part, also hosted trust and security R&I project cluster activities of SecCord.

The second can move forward from these two meetings to decide the details of its responsibilities and modus operandi answering the question posed above, and in general,

> *how best to work together for maximum benefit to the research and innovation projects and to the programme as a whole?*

The third –*NIS cluster*– although outside the scope of these meetings, it is envisaged that its operation will almost certainly involve the other two clustering processes.

The main outcome of the morning session was the presentation of the projects' objectives, expected results and mapping of timelines, and the examination of potential commonalities and specialties of the projects. A number of these were identified from the participating partners as shown in the table given below.

[4] http://fisa.future-internet.eu/index.php/Main_Page

A further analysis of this data was undertaken in the afternoon meeting, with follow up actions for the participants.[5]

A number of topics resonated throughout the presentations of the morning session as ways of increasing impact, principally:

Research roadmaps: an activity for several projects; therefore, we should examine how work can be aligned and coordinated;
Focus on excellence: focus on areas where the EU has recognised leadership and competitive advantage: e.g. cryptography, biometrics, smart card and smart grid, etc.;
Sharing information: clusters should maintain visibility and accessibility of project results and insights for longer, so they do not simply disappear at the end of a project;
Learning lessons: using the cluster to gather lessons learned (good and bad) from projects, which are usually never captured anywhere;
Risk management: bringing together projects involved in developing multi stakeholder approaches to risk management for trust, security and privacy.

3 Workshop Sessions

All the current CSAs and NoEs, together with the recently completed ECRYPT II NoE, took part in two sessions during CSPF 2013. The CSP Track 14 session was part of the general workshop agenda. It consisted mainly of presentations of the goals and timescales of the CSAs and the projects' answers to questions looking at current objectives, outputs, planned events and interactions, relation to current European policies for cyber security, and possible structure for a NIS Platform and ways that the CSAs and NoEs – and the research and innovation projects – might participate and contribute. The presentation details, answers to the questions, together with the commonalities and niche specialties of the CSAs that were examined were captured in a comprehensive CSP Forum 2013 *Track14* report [4, 5].

The purpose of the follow-on afternoon meeting between the CSAs, the NoEs, and DG CNCT Unit H4 was to look in further detail at options and possibilities for the structure and modus operandi of project clustering, and ways forward towards a NIS Platform. A number of desirable clustering attributes were identified. These include extending their participation, influence, and effect to projects outside the immediate ICT trust and security community, particularly those concerned with legal, economic, health, and social focus, where there is an inherent need for security of information and infrastructure. Not least is the requirement for continuity of the project clusters so that the legacy and achievement of projects is not immediately lost on their completion; one of the difficulties has arisen from the batch profile of a particular Call for Proposals, so that work from earlier calls, e.g. FP7 Call 1 with its Identity Management objectives, say, seems all but forgotten by the time of later calls, although results and issues are still valid and valuable.

[5] The full slide sets of the speakers are available from http://www.cspforum.eu/uploads/14_NetworkingCoordination.zip

3.1 Agenda Track 14 Workshop

The purpose of the morning clustering session was

1. to identify requirements for clustering to ensure a well-coordinated approach for the industrial cyber security strategy in the EU and beyond;
2. for CSAs and NoEs to present their core objectives, specialty areas of coverage, synergy with other projects, and relation to current major EC actions;
3. to identify common interests and potential synergies that can be exploited to set up a coordinated approach for clustering;
4. to discuss and gather feedback from participants on where the CSAs/NoEs can potentially support the setup of NIS platform.

In order to maintain focus, the projects were given a structured template in which they presented their coverage areas and specialties, in terms of: objectives, challenges, timeline; outputs, and synergy with other projects; relation to current major European Commission policy actions; and vision of NIS Technology platform infrastructure. The table below summarises the identified *commonalities* and *specialties* of projects.

This presented material and subsequent discussions provided valuable input to the follow-up meeting held in the afternoon.

3.2 Follow-Up Meeting

The purpose of the afternoon session was to explore some of the functional and operational requirements of project clusters, particularly concerning cluster-coordination, and possible need to support NIS – or other future *targeted* initiatives. The main outputs are discussed in Sect. 4 below, and listed in full in the Appendix. Discussion between the projects and EU representative arrived at a recommended framework for clusters.

General Coordination Cluster. The functionality of the cluster (in common with other envisaged clusters) –and hence *deliverables*– would concern:

– *policy support* for cyber security and information protection;
– *cluster dissemination*: cluster website, cluster book, cluster identity, spreading excellence;
– *conference and event planning*: thematic tracks for publication, joint conferences and workshops;
– *research roadmap*: strategic research agenda, cyber security innovation plan, standardization plan.

NIS Cluster Functional Structure. The basic framework of the NIS support cluster would provide: cluster secretariat; cluster coordination; EU contacts and liaison; activity coordination; three expert Working Groups (currently being established).

This might be set up as a specific ad hoc structure, or could be sourced from one or more of the available members of the General Coordination Cluster. The cluster activities could lead on to a more extended European Technology Platform (ETP).

Table of project commonalities and specialties	NESSoS	STREWS	CIRRUS	ATTPS	FIRE	SysSec	CYSPA	ECRYPT II	BIC	SECCORD
Cloud computing – security certification, internationalisation, standards	☑	☑	☑	☑	☑				☑	
Research agendas	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Web services security road-map		☑								
Dissemination expertise	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Participatory methods e.g. running Advisory Boards, Working groups, Clusters	☑	☑		☑	☑	☑	☑		☑	☑
Establishment of platforms/ infrastructures for cooperation	☑			☑	☑	☑	☑		☑	☑
Repository/platform for dissemination/sharing information		☑	☑	☑	☑	☑			☑	☑
Enabling technologies e.g. Cryptography	☑			☑		☑		☑		
Services and software engineering security	☑	☑	☑							
Building International cooperation (INCO) via road mapping and models									☑	
INCO in terms of involvement of non EU countries		☑	☑	☑	☑	☑		☑	☑	
Policy analysis and support (e.g. for H2020, cybersecurity, NIS platform, …)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Education: summer-schools etc.	☑					☑		☑		
Linkages with industry and industrial sectors	☑	☑		☑	☑	☑		☑		☑

4 Workshop Recommendations and Proposals

The workshop arrived at a number of findings or proposals for future action regarding Trust and Security project clustering. These are given in full in [4], but included here for completeness as an Appendix. Below we attempt to summarise and consolidate them into a small number of groups, and discuss briefly the implications arising. The conclusions and overall recommendations and goals are then given in Sect. 5.

4.1 Overview of Grouping of Recommendations

The workshop recommendations can be allocated into four inter-linking groups outlined below.

Membership: the conditions and qualifications of membership, and the challenges of ensuring involvement by all (H4) T&S projects, and extending participation to the wider community of framework projects and beyond.

New work items, content, and cluster initiatives: the nature, content and priorities of the work to be undertaken by the project clusters.

Organisational and administrative: mainly about possible evolution of EU procedure to formally support the formation and operation of *project clusters*.

Cluster operations: how the clusters should be organised – and organise themselves – to undertake collaborative work and to contribute to collective activities, such as, currently, the annual CSP conference, and, in the future, shaping the programme and policy, and inputs to the NIS initiative.

4.2 Disposition and Discussion of Workshop Recommendations

This section looks at the groups of recommendations and seeks to provide pointers to future action. The assumption is that Project Clustering can and should be beneficial:

– the underlying questions concern *what*? and *how*?

MEM – Membership
(items labelled MEM in Appendix)
Membership of T&S clusters should be free of charge, in that there should be no direct joining or contributory participation charges; however, clustering activities do not come for free, and there needs to be either funding allocated in project budgets (in Grant Agreements), or there should be some form of centrally allocated budget, possibly channelled through a nominated project. Currently, the cost of participation is generally 'found' from some squeeze or underspend within existing project budgets. (see also *ORG*, below).

Cluster participation should be extended by invitation to all projects with an interest, dependency, or commitment, relating to trust and security. The more obvious fields would include health and welfare, economics, legal, societal, infrastructures (physical services, transport and communications, and underlying administrations, etc.), some of which come under the Security Research programme.[6]

Work Items, Workplan, Content
(items labelled NWI in Appendix)
There are four principal aspects to the work of the clusters: *technical cooperation and collaboration*; *dissemination and communication*; *community building*; and *contribution to cyber-security policy and planning*. In addition there may be, from time to time, special assignments from the Commission.

The scope and content of the technical work should be decided by the cluster participants taking into account their own interests together with the needs of the overall EU [cyber] trust and security programme and initiatives.

There is an urgent need to get the clusters active, following an inclusive plan. The intention is for the NoEs and CSAs to form a sort of *programme committee*, chaired by SecCord. In general, the work should build on EU strengths in areas such as cryptography, smart card, embedded systems, biometry, privacy, but recognizing the projects own commitments. The clusters could also provide a lookout, monitoring

[6] http://cordis.europa.eu/fp7/security/

gaps or weaknesses, and giving warnings of technical or economic vulnerabilities, as many projects are committed to this type of activity anyway.

Dissemination and communication activities are addressed mainly under *Cluster operations*, below, about events and communication channels, however, it is suggested that a component of technical collaboration would be producing forward-looking research white-papers on challenges and achievements.

Community building has two dimensions: strengthening the cohesion within the clusters; and extending visibility and awareness within the programme and externally to other EU entities, and into Member States. This extension has always been a problem: the annual CSP conference does provide a platform to a potentially wider audience, but getting beyond the *usual suspects* does remain a challenge. The Commission should be able to provide support with contacts and active participation.

As an input to policy and future planning, CSAs have had a tradition of producing roadmaps that contribute to the forward *Strategic Research Agenda*. The clusters provide a valuable mechanism for coordinating and integrating this work, with further opportunities for mechanisms for searches, *views*, digests. The above white papers, particularly the *kite-flyers*, can also add value here.

Organisational and Administrative – Mainly EU Procedure

(items labelled ORG in Appendix)

Two main points were made concerning the role of the Commission, and more particularly Unit H4, responsible for trust and security.

The first concerns the material support for clustering, and its formal recognition and funding. The participation in clustering is actively encouraged by Unit H4; however, other than some budget in the CSAs to cover organisational matters, there has been no R&I project budget nor work package commitment formally allocated to cluster participation to date. The question is raised whether there can be any revision to current DoWs, and whether future Grant Agreements should make provision (automatically) for cluster participation.

The second point concerns active participation in, and support of project clustering by the Commission. Unit H4 is already active in promoting the importance of ICT trust and security: that the programme as a whole – and its participants –should be as much cyber-security aware as it is cyber-aware. However, it is suggested that universal cluster membership should be mandated as strongly as possible, and that optimum use should be made of current CSAs and NoEs by ensuring full collaboration – again by strong encouragement where brute force may not be actually possible. Future provision for clustering should recognise the need for appropriate coverage by CSAs, with the possibility for flexible movement of responsibilities between them.

As noted earlier, it would be most helpful for the Commission to provide the contacts and introductions to beyond the immediate area of cyber Trust and Security.

Cluster Operations and Support

(items labelled OPS in Appendix)

The main topics here concern dissemination and communication, and their channels; and activities supporting other project cluster operations. These include activities and responsibilities that may already fall naturally within the remit of existing CSAs (see

Table given above), but could be extended and strengthened through their further collaboration and cooperation.

Dissemination concerns the sharing and publication of content arising from the cluster projects: their results and ideas – as individual projects, and from cluster collaborations. One aspect is communication with the immediate Trust & Security (technical) community; the second is communication with other research bodies and industry, and with the policy and decision makers of the EU and *current/future/planned* initiatives such as H2020, NIS, and Directives.

The channels that project clustering can provide are a common website (*Cyber Security and Privacy*, say, as already established for the CSP conference), and cluster workshops and conferences.

The website should provide communal cluster and individual projects spaces to provide not only access and visibility to the CVs and prospectuses of projects and participants, their results and achievements, and cluster event news and reports, but also to provide for sharing of more speculative ideas and challenges (*kite-flying*, as above). Ideally, the whole set of information could be seen as a structured, searchable library of Trust and Security news, concepts, technical outcomes and policy contributions (such as roadmaps). It could also provide a valuable directory to other sources of news, events, and information. The cluster could also make use of other social media outlets, as appropriate, e.g. LinkedIn Group, Twitter, …

Cluster workshops and conferences should address big-picture *themes* and concepts as well as specialist, detailed-picture *topics*. Successful events of these sorts have, of course, been held previously, but a coordinated cluster approach should be able to add further value to the quality of content and communication of outcomes.

For example, an annual publication could go beyond this set of CSP conference proceedings (as here, that could provide a valuable foundation and approach); it may need to extend beyond a single volume if it were to incorporate leading results and discussions from the Trust and Security community.

An ongoing challenge for cluster dissemination and communication is how to reach out to those *outside* the Trust & Security community itself, not least to the areas of the programme that have inherent or implied Trust & Security issues or dependencies (e.g., health, transport, legal, economic, infrastructure, as in *Membership*, above). The challenge of getting them to actively participate – with presumably limited funding, scope, and direct references in their DOWs – is, of course, something that needs to be overcome and would need direct support from their constituent funding authority and project officers.

Activities supporting other project cluster operations mainly concern planning and coordination: the management of cluster events; establishment and maintenance of a work programme; integration of, for instance, the roadmapping work of individual projects, and creating a unified structure with identifiable scope, commonalities, overlaps, and gaps.

5 Conclusions and Goals

The longer term continuation and extension of Trust & Security project clustering is seen as potentially beneficial and effective if structured correctly: for the individual projects; and for the trust and security aspects of the Framework Programme.

Immediate next steps should be

- to start building the cluster community, including addressing the administrative, scope, promotion, and structure questions to address the challenges as outlined for existing, new and future projects;
- to build web presence and visibility;
- to compile the CSPF book – selected proceedings including this paper to share with a wider audience (published summer time 2013);
- to generate a calendar overview of relevant events.

Acknowledgements. The participating projects are supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security;
http://cordis.europa.eu/fp7/ict/security/home_en.html
SecCord is supported under Grant Agreement No. 316622.

A.1 Appendix – Workshop Recommendations

(MEM) – membership; (NWI) – new work items, content, initiatives;
(ORG) – organisational; administrative; (OPS) – cluster operations

R1. Membership of the Trust and Security Project Clusters should be open to all Framework Programme projects; those outside Trust & Security itself that have inherent or implied Trust & Security issues would be most welcome (e.g., health, transport, legal, economic, infrastructure, …). (MEM)

R2. Membership of clusters should be free; a project will coordinate the cluster activities and, if necessary, Descriptions of Work (DOWs) should be examined and changed if necessary to align a project's tasks with the responsibilities taken up in the cluster.
Note: The SecCord (CA) project already has such cluster coordination responsibilities in its objectives; it could act as a "contact point" for the cluster community. (MEM)

R3. The cluster of CSAs/NoEs should make a start on areas that are more concerned with community building (e.g. conferences, workshops, research roadmaps …).
Note: Assistance from the Commission will be needed to provide contact points and short descriptions of all projects, especially those in new Calls. (NWI)

R4. The Unit H4 Trust and Security should be take part in the cluster activities, and should strongly encourage its projects to play an active role in the clusters. (NWI)

R5. In order to provide continuity through H2020 (and even beyond), clusters should have a span beyond a set of projects arising from a single call; responsibilities in the clusters and allocations of activities may change over this lifespan, partners in newly-funded projects taking over tasks from completing projects. (ORG)
R6. The Commission should also consider the need for specific cluster-supporting project(s) when drafting future calls. (ORG)
R7. Cluster priorities should be the responsibility of the cluster-members themselves, but taking full account of the requirements of such as the Cyber Security Strategy, the NIS platform, the societal pillar in H2020, etc. (NWI)
R8. There should be provision for rotation of certain periodic responsibilities to lessen the burden on some projects e.g., hosting meetings, organizing sessions, specific work activities required. (ORG)
R9. The appropriate stakeholders (people/projects/initiatives) should be brought together to begin scoping cluster activities, to get active membership, and to gain agreement on who does what and when. There should be draft plan for 2013 cluster activities, with allocated responsibilities, available for the next cluster meeting. (NWI)
R10. Earlier and current cluster models should be reviewed, e.g. Effectsplus, SecurIST, PRIMCLUSTER, GEANT, IN-HOME, etc., to see how they have been organized, their benefits and/or problems encountered. (ORG)
R11. Clustering should be supported by all Trustworthy ICT projects. A number of coordination and support activities in the security domain already have some associated cluster activity that they should look with a view to taking on further clustering responsibilities. (ORG)
R12. The clusters should build activity streams around EU strength areas: e.g. cryptography, smart card, embedded systems, biometry, privacy, and others. (OPS)
R13. The cluster should examine benefits and possibilities for collaboration on utilising summer schools of the projects. (OPS)
R14. Similarly, the cluster should look at possibilities for theme-based conferences/workshops: a continuous effort in order to share data, capitalizing in the "scale effect" of a big cluster for small companies could be provided. (NWI)
R15. The cluster should encourage white papers, to be made available in a central featured repository (as in BIC), in which authors are invited to submit articles via the projects, keeping in mind that the basic data sometimes comes in a fairly rough format and the responsible project compiles into a nice glossy format for publication. (OPS)
R16. The clusters should be used as a vehicle to promote the trust and security message and promote it as a central consideration for all projects. The audience is our community, including the European Commission, research, industry, policy, decision makers (and eventually NIS platform). (OPS)

R17. There would ideally be an annual book from the clusters. (possibly along the lines of this CSP Forum volume; another example was the yearly FIA book). The annual trust and security book should take care to support the identity of the trust and security clusters (of course, it also links in the Future Internet, telecommunication, mobile, smart grid, and many other topics, but the competence of the trust and security community should be the dominant contributor. (OPS)

R18. Each project that is a member of the Trust and Security cluster should put an executive summary on-line on the cluster web platform. The choice for the web platform has not yet been made but the CSP forum would be a candidate. There should be formal agreement from all projects to communicate their public deliverables to the cluster website; the cluster website should be a collaboration platform that offers broad functionality to the cluster members (e.g. to upload deliverables themselves, to update entries in the cluster agenda, to release news items, …). (OPS)

R19. Research agendas/roadmaps should be catalogued. (OPS)

R20. There should be a directory or atlas of roadmaps, taking into account the diversity of the various topics. They could use the rendezvous concept, where the roadmaps have been analysed and points of contact determined so that matters may be coordinated along technology (or other) lines. (OPS)

References

1. 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. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
2. 2013/0027 (COD) Proposal for a directive of the European parliament and of the council concerning measures to ensure a high common level of network and information security across the Union (e.g.,) http://www.europarl.europa.eu/oeil/popups/summary.do?id=1247517&t=d&l=en
3. Minutes of the NIS Platform Kick-off meeting held 17th June 2013 in Brussels
4. NoE & CSA Clustering Report – CSP EU Forum 2013. http://www.cspforum.eu/uploads/CSP_Track14_Report.pdf
5. Track 14 presentation material: Networking and Coordination cluster of CSAs in Trust and Security; Chair: Jim Clarke, Waterford Institute of Technology (TSSG); within Presentations Day 2. http://www.cspforum.eu/2013/programme/presentations-day-2

Author Query Form

Book ID :	**319378_1_En**
Chapter No.:	**12**

Springer
the language of science

Please ensure you fill out your response to the queries raised below and return this form along with your corrections

Dear Author
During the process of typesetting your chapter, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

Query Refs.	Details Required	Author's Response
AQ1	Please check and confirm the affiliation details for the author C. Bodeau-Pean is correct and amend if necessary.	

MARKED PROOF

Please correct and return this set

Please use the proof correction marks shown below for all alterations and corrections. If you wish to return your proof by fax you should ensure that all amendments are written clearly in dark ink and are made well within the page margins.

Instruction to printer	*Textual mark*	*Marginal mark*
Leave unchanged	··· under matter to remain	
Insert in text the matter indicated in the margin		New matter followed by or
Delete	through single character, rule or underline or through all characters to be deleted	or
Substitute character or substitute part of one or more word(s)	through letter or through characters	new character or new characters
Change to italics	under matter to be changed	
Change to capitals	under matter to be changed	
Change to small capitals	under matter to be changed	
Change to bold type	under matter to be changed	
Change to bold italic	under matter to be changed	
Change to lower case	Encircle matter to be changed	
Change italic to upright type	(As above)	
Change bold to non-bold type	(As above)	
Insert 'superior' character	through character or where required	or under character e.g. or
Insert 'inferior' character	(As above)	over character e.g.
Insert full stop	(As above)	
Insert comma	(As above)	
Insert single quotation marks	(As above)	or and/or or
Insert double quotation marks	(As above)	or and/or or
Insert hyphen	(As above)	
Start new paragraph		
No new paragraph		
Transpose		
Close up	linking characters	
Insert or substitute space between characters or words	through character or where required	
Reduce space between characters or words	between characters or words affected	