EUROPEAN COMMISSION
JOINT RESEARCH CENTRE
Institute for the Protection and Security of the Citizen
Global Security and Crisis Management Unit

Date: 14.01.2013
Action: OPTIMA

Open Source Information Capacity Support

Interim Report 01/2013

Administrative Arrangement

Between

DG Home Affairs (DG HOME)

No. HOME/2010/ISEC/AA/003-A1, ABAC No 30-CE-0444512/00-75

and

Joint Research Centre (JRC)

JRC No. 31992

Document History

Date	Author	Comments
14.01.2013	[redacted]	Initial draft
22.01.2013	[redacted]	Small revision
06.02.2013	[redacted]	Included comments from DG HOME

1 OVERVIEW

This document gives an update on the progress of work done towards the goals of the Administrative Arrangement "Open Source Information Capacity Support". Furthermore, it contains an updated project plan for the next phase of the collaboration.

2 EXECUTIVE SUMMARY

Progress on the defined work packages has proceeded as planned. The following milestones are completed:

- Training and installation of EMM at DG Home's premises
- Support for EU Anti-Corruption Report
- Four incremental versions of EMM OSINT Suite with lot of functional additions delivered to law enforcement users (20 software licenses signed)
- Three OSINT workshops (2 hands-on workshops and 1 expert forum) organised with high interest from the MS law enforcement community
- Community website ported to new technical platform

The following work packages will be completed in 2013:

- Continuous EMM support to MS authorities and DG HOME's analytical capacity
- Further releases of EMM OSINT Suite desktop toolkit
- Online version of OSINT Field Guide as content for the community website

Currently, no major challenges are known which could impact the delivery of the remaining open tasks.

3 WORK PACKAGES OVERVIEW

This chapter gives a brief overview of the different work packages of the AA. The list of packages forms a reference for the description of the performed work and the updated project plan as described in subsequent chapters. For a full description of each individual package and overall background information please refer to the Technical Annex of this AA.

The first goal of supporting DG HOME's information gathering capacity is defined in chapter 3.1 of the technical annex. It is further structured into the following work packages:

Work Package 3.1.1: Support to DG HOME's Crisis Management and Information Gathering Capacity

M1 (Milestone 1): Create EMM Monitoring Categories

Create categories in collaboration with DG HOME to monitor sources of EMM for DG HOME's areas of interest

M2: EMM Training

Train DG HOME's staff on site in Brussels with access to the EMM NewsDesk editorial interface to compile information products.

M3 (optional): Full Installation of EMM at DG HOME

Provide a full installation of EMM at DG HOME's premises to allow fully autonomous use of EMM applications during a crisis situation.

Work Package 3.1.2: Compilation of information for the planned EU Anti-Corruption Report

This work package relies on milestones delivered by the preceding work package.

M4: Setup EMM Account

Creation of an EMM account for DG HOME's unit A.2 to compile information on relevant prominent corruption cases on a periodic basis for all 27 EU MS.

M5: EMM Training for Duty Officers

Provide at least one day of training to DG HOME duty officers in Brussels on the use of EMM applications.

The second goal of improving member state capabilities by disseminating and improving existing tools is defined in chapter 3.2 of the technical annex. It is further structured in the following work packages.

Work Package 3.2.1 OSINT Community and Tools

M6: Continuous Development of EMM OSINT Suite

Provide at least 2 feature releases per year of the EMM OSINT Suite software in response to user requests.

M7: OSINT Field Manual

Create online OSINT Field Manual describing best practices of using OSINT for law enforcement purposes.

M8 (optional): Printed OSINT Field Manual

Create a printed version of the OSINT Field Manual.

M9: OSINT Workshops

Organise in total four workshops for law enforcement professionals about OSINT tools and techniques. (One workshop may be collocated with the workshop as defined by M10).

Work Package 3.2.2 EMM Server Suite

M10: EMM Information Workshop

Organise a workshop for MS authorities to present the provided EMM server applications.

M11 Initial EMM Server Setup for Member State

Provide initial setup of an EMM Server installation as requested by a MS.

M12: EMM training for Member State staff

Provide basic training for Member States' staff on how to operate the EMM installation.

Reporting

M13: Inception Report

Submit inception report within one week after kick-off meeting, describing project plan for the first 6 months, team composition and further results of kick-off meeting.

M14: First Interim Report

Submit draft of interim report within 6 months of AA execution containing executive summary update on carried out activities, progress report with results and difficulties and interim findings and conclusions on work packages 3.1 and 3.2. Submit revised final report within fourteen days of receiving DG HOME's comments.

M15: Second Interim Report

Submit draft of second interim report within 15 months of AA execution addressing the same topics as first interim report. Submit revised final interim report within fourteen days of receiving DG HOME's comments.

M16: Final Report

Submit draft of final report within 22 months of AA execution containing a description of the work accomplished and results obtained. Submit revised final report within fourteen days of receiving DG HOME's comments.

4 PROGRESS REPORT BY MILESTONE

This chapter gives an update on the work performed until the 14th of January, 2013. We structured this update according to the defined milestones.

Work Package 3.1.1: Support to DG HOME's Crisis Management and Information Gathering Capacity

- M1: Support to DG HOME staff related to definition, creation of EMM monitoring categories was provided.
- M2: Two online training sessions for DG HOME personnel were performed via phone conference

Work package 3.1.1 included an optional milestone M3 which contained a dedicated installation of EMM server at DG HOME's premises. This milestone has been moved into a dedicated AA[1] with DG HOME which also comprises additional elements not covered by this AA.

Work Package 3.1.2: Compilation of Information for the planned EU Anti-Corruption Report

- A list of existing relevant categories has been forwarded to DG HOME
- M4: A dedicated EMM NewsDesk and AlertEditor account has been created
- In close collaboration with DG HOME's analysts further category definitions have been added to the system covering topics important for the Anti-Corruption Report.

[1] N° HOME/2011/ISEC/AA/002-A1, ABAC N° 30-CE-0513429/00-84 N° JRC.32848-2012 NFP

Work Package 3.2.1 OSINT Community and Tools

- M6: The EMM OSINT Suite has been further developed and four major releases of the software were released to users. In addition a set of patch releases were provided to fix smaller issues.

- Improvements comprise:

    - Information extraction modules

        - Text extraction supports additional binary input formats (MS Office 97, 2007, Open Office)

        - Entity extraction pipeline completely revised for more performance

        - Name variant database pre-filled with name variants gathered from EMM

        - Import and export name of variant data

        - User defined custom entity types based on a powerful new pattern engine

    - Web Search module

        - New predefined search engines added (Yahoo.com and Blekko.com)

        - Addition of user defined search engines simplified

    - Analysis modules

        - New entity browser component to browse the extracted entity information more effectively

        - Revised graph analysis view integrating with the entity browser component

        - Enhanced report generator

    - Support for latest MS Windows 32-bit, 64-bit and Apple OS X operating systems

Most of the new functions, such as the entity browser component, were developed based on direct feedback from users in the law enforcement community.

Due to demand from users an updated version of the v1.3 development stream of the software was released in early 2012. The purpose was to extend the operational lifetime of this version and to provide more time for users to upgrade to the v2 version of the software.

To date 20 MS authorities have licensed the OSINT Suite software package as listed in the annex.

- M7: The literature research phase of the OSINT Field Manual has been concluded and a draft of the manual is going to be published on the OSINT Community Website in Q1/2013. Work on this field guide was pushed back in order concentrate first on improving the OSINT Suite software more rapidly. Also, this provided more time to test the new technical platform which forms the basis for the community web site going forward.

- M9 OSINT Workshops

    - The first OSINT workshop took place in October 2011. This event provided hands-on exercises with our software tools.

- The second OSINT workshop took place on the 21.-22. June 2012. This event was organised as an expert forum containing presentations from OSINT experts in the MS. One of the main topics was the use of social media for investigative purposes. This event was fully booked which shows the high interest from the law enforcement community. Please refer to the annex for a list of the given talks with short abstracts. The complete presentations can be found on the OSINT Community web site.

- The third OSINT workshop took place 27.-28. October, 2012. This event provided hands-on exercises with our software tools. Again, this workshop was very well received with over 30 participants from EU institutions and MS. Please refer to the annex of this report for the agenda of this event.

- The fourth OSINT workshop is planned to take place in April, 2013. This event is planned as an expert forum with presentations from OSINT experts in the MS. An official announcement will be sent out in January 2013.

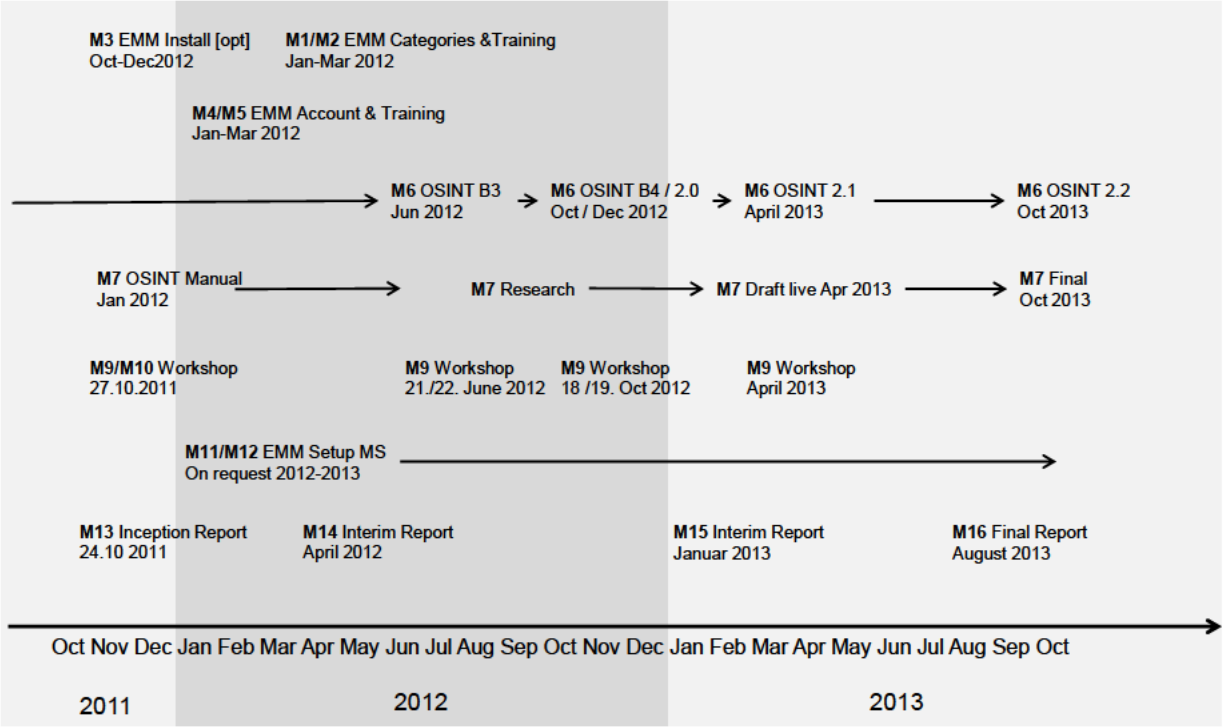
Please refer to the annex for the agendas of the different workshops and information about participation from the MS.

Work Package 3.2.2 EMM Server Suite

- M10: An EMM Information Workshop was organised in October 2011. 40 participants from MS law enforcement authorities and EU institutions took part.
- M11: Members of the project team visited the Dutch Internet Service Centre in order to support them operating an EMM installation which serves Dutch tax and law enforcement authorities. An installation with the Dutch customs is going to be used as a prototype for Dutch, French and British customs. Additionally, Swedish customs and Romanian authorities expressed interest in dedicated EMM installations.
- The following MS institutions were provided with an account on EMM NewsDesk to allow them to evaluate the system:
    - Belgium Ministry of Finance / Tax Office
    - Belgium Security Service VSSE
    - Europol
    - Estonian Police
    - DG HOME
    - Slovenian Police
    - Swedish Police

5 Project Plan Update

The following diagram shows the updated project plan with deliverables as described under the respective milestones.



Most of the milestones have been completed as planned to date. Some work packages are still on-going, such as EMM support to Member States. For the development of the OSINT Suite tool set we plan two major releases in 2013 with new functions and a number of patch releases correcting minor problems. The expert forum workshop in 2013 is planned for late April. The reason is that a date in June is difficult for participants from the Scandinavian countries because of the public midsummer holiday. In May there are a number of public holidays across the EU which makes it also difficult to find a suitable date. Therefore, the best option is to bring the workshop forward to late April. The launch of the OSINT Field Manual has been postponed to the first quarter of 2013 which provided more time to test the new technical platform for the community web site. Apart from this change the project plan is on track and all work packages will be delivered in the remaining time.

6 Project Plan Assessment

The team composition changed at the end of June 2012, with [redacted] leaving the project. This impacted the first public version of the OSINT Field Manual. The launch was further postponed since the new technical platform for the community web site needed extensive testing. By shifting more resources to it we are confident to launch the first public version in the first quarter of 2013. For the other open work packages we see no major challenges.

7 Annex

The annex contains the following additional information:

- Agenda Workshop October 2011
- Agenda Workshop June 2012, Presentation abstracts

- Agenda Workshop October 2012
- Licensed users of EMM OSINT Suite

7.1 Agenda Workshop October 2011

The first workshop was co-located with the EMM Information Day as defined by milestone M10. The event took place 27.-28.10.2012. The event was fully booked with 40 participants from across Europe.

7.1.1 Thursday, 27.10.2011

- 09:15 Welcome Remarks, [redacted], DG HOME
- 09:45 EMM Suite of Tools – Overview, [redacted], JRC
- 11:00 EMM Server Interactive Session 1
- *Lunch Break*
- 14:00 EMM OSINT Suite 2.0, [redacted], JRC
- 14:30 Monitoring Media for Events: Moving from Early Alerting to Early Warning, [redacted], JRC
- 15:30 EMM Server Interactive Session 2
- 17:00 EMM Server Interactive Session 3

7.1.2 Friday, 28.10.2011

- 09:15 Welcome Day 2

Parallel Sessions:

- 09:30 EMM OSINT Suite – Acquisition & Basic Functions
- 11:00 EMM OSINT Suite – Advanced Functions
- 09:30 EMM Server Interactive Session 4
- 11:00 EMM Server Interactive Session 5
- 12:15 Closing Remarks, Feedback, Wrap-Up

7.2 Agenda Workshop June 2012

The June workshop was organised as an expert forum with presentations from experts across Europe. The event was fully booked with 44 participants from across Europe.

7.2.1 Thursday 21 June 2012

- 09:15 Welcome remarks DG Joint Research Centre, [redacted], JRC

- 09:25 Welcome remarks DG Home Affairs, [redacted], DG HOME
- 09:45 Open source intelligence – a practitioner's perspective, [redacted] (Research Manager, West Midlands Counter Terrorism Unit, United Kingdom)
- 11:15 Real-time intelligence during events, [redacted] and [redacted] (Senior information analysts, Regional Police, Netherlands)
- *Lunch break*
- 14:00 Romanian Muslims on social platforms, [redacted] (OSINT expert, Romanian Intelligence Service, Romania)
- 15:30 Public and private data analysis using open-source components in the real world with the iColumbo project, [redacted] (Lead Developer of iColumbo/Founder of Seajas, Netherlands)
- 16:30 Feedback and conclusions

7.2.2 Friday 22 June 2012

- 09:10 Opening workshop
- 09:15 How to improve security of police databases, [redacted] (Police Superintendent, General Police Directorate, Slovenia)
- 09:45 Internet surveillance in practice, [redacted] and [redacted] (Internet surveillance, Regional Police, Netherlands)
- 11:00 The challenges of applying social network analysis to social media, [redacted] (Intelligence Team Manager, Verisign iDefense, United Kingdom)
- 12:00 Feedback and conclusions
- 12:20 Closing remarks DG Home Affairs, [redacted] (Head of Sector, Strategic analysis and response, DG Home Affairs, European Commission)

7.2.3 Presentation Abstracts

- [redacted] - Research Manager, West Midlands Police Counter Terrorism Unit, United Kingdom

  Open source intelligence - a practitioner's perspective

  The presentation will cover a brief history of the Counter Terrorism Unit and its functions, followed by an overview of how the OSINT capability has been developed highlighting some of the issues, pitfalls, some of the solutions and the future. The presentation will contain examples of how OSINT assisted investigations including one case that led to a successful conviction.

- [redacted] / [redacted] - Senior information analysts, Regional Police Force, Netherlands

  Real time intelligence during events

During events, social media is scanned for signs of public disorder. Based on these signals, management information is produced. With this intelligence, police commanders are more able to give instructions to their police officers. In this presentation, examples and methods are discussed on the basis of the following three events: a demonstration of activists, a football match and the Dutch national celebration day “Queen’s Day”.

- [redacted] - OSINT expert, Intelligence Service, Romania

Romanian Muslims on social platforms

The communication changes registered by extremist organizations triggered a specialized approach in terms of monitoring the virtual space, in other words an appropriate management of the investigation results by means of an automated Social Network Analysis and Sentiment and Affect Analysis.

Given radicalization and self-radicalization high risks, security agencies need to establish the exact nature of an online social network by monitoring both quantitative elements (network dimension and volatility, frequency of participation in debates, number of messages per time unit) as well as qualitative issues (position of each member within the network; issuers’ persuasive ability; discourse patterns; indoctrination level and radical transformation potential).

The lack of a violent discourse inside a social network, although extremely convenient for security organizations, could actually be just a cover for achieving Islamic extremism main goal – setting up an Islamic conscience to precede the establishment of the Caliphate, based on rooting out Western influences and the practice of the ‘right’ religion, in European Muslims’ case.

In this particular context, one should use semantic analysis tools to explore a virtually unknown zone, namely translate human emotions into measurable data by resorting to sentiment analysis filters (positive versus negative), in order to reveal their intensity (level of emotional expression), clarifying the evolution of the radicalization process by which a moderate individual or group comes to adopt radical ideas and disseminate them.

The study I will present to you right now reveals the interest in using social media in order to strengthen the ties within the community and exchange almost radical opinions. Seeds of an inflexible form of Islam have been noticed, the trend being visible especially among young native and converted, who, driven by the need to be fully accepted by their adoptive ’family’, eagerly take part in activism projects.

- [redacted] - Lead Developer of iColumbo/ Founder of Seajas, Netherlands

Public and private data analysis using open-source components in the real world with the iColumbo project

Data gathering, both on the public internet and from private sources, provides insight and relevance to intelligence and public institutions alike. With tangible implementations in the real world, we've built and used open-source components to provide search and data analysis capabilities that prove that these systems can be built using transparent open-source software and technical systems.
One of these implementations — part of the IRN / iColumbo Internet Monitoring project — focuses specifically on meeting the stringent privacy and security requirements set by public institutions. Its open and transparent design makes the technology suitable for democratic

and legal review as well as meeting forensic standards to make the information suitable to be used as evidence in court cases.

- [redacted] - Police Superintendent, General Police Directorate, Slovenia

  How to improve security of police databases

  A large amount of data in log files can keep track of user's activities in police databases. Examination of these log data for insider abuse can be a hard work. This presentation is aimed at our approach to support the examination of the log files.
  We support the examination by a recommender system that combines internal and external data in order to identify suspicious patterns and items. The identification is based on various data analysis techniques, from simple queries to advanced data visualization techniques and assessment models. The recommender system is composed of KNIME open source platform for data analyses, and data gathering tools such as OSINT Suite.
  The presentation will be focused on integration between the OSINT Suite and the KNIME platform. The OSINT Suite provides additional data from public sources that can enrich log file data, and the KNIME integrates this data into the recommender system. This concept can also be used for examination of similar data such as emails and various documents.

- [redacted] / [redacted] - Internet surveillance, Regional Police Force, Netherlands

  Internet surveillance in practice

  This presentation focusses on who we are, what we use and some examples of internet surveillance and investigation in our police region.

- [redacted] - Intelligence Team Manager, Verisign iDefense, United Kingdom

  The challenges of applying social network analysis to social media

  One of the most powerful tools in the social scientists tools box is Social Network Analysis (SNA), a method that can reveals hidden meaning in otherwise formless social groups. SNA has been successfully applied by intelligence agencies for decades into mediums such as telephonic analysis and the social hierarchies of numerous criminal and terrorist groups. Can SNA be as effectively applied to the medium of cyber space, specifically the social groups active within online forums and chat channels? This talk examines both the pitfalls and possible solutions to applying SNA to the cyber medium.

7.3 Agenda Workshop October 2012

The second workshop in 2012 was organised to contain hands-on sessions about our OSINT tools. The event was well received with 30 participants. The sessions took place in two parallel tracks covering an end-to-end scenario with EMM NewsBrief and basic and advanced sessions with EMM OSINT Suite.

7.3.1 Thursday, 27.10.2012

- 09:15 Welcome Remarks, [redacted], DG HOME
- 09:30 Welcome Remarks, [redacted], JRC
- 09:45 EMM Products Overview & Latest Research

- Event Extraction, [redacted], JRC
- Twitter Mining, [redacted], JRC
- Automatic Summarisation, [redacted], JRC
- Sentiment Detection, [redacted], JRC

- Parallel Sessions
- 11:15 EMM End-to-End 1
- 11:15 EMM OSINT Suite Web Search, Crawling, Data Import
- *Lunch Break*
- 14:00 EMM End-to-End 2
- 14:00 EMM OSINT Suite Entity Extraction
- 15:30 EMM End-to-End 3
- 15:30 EMM OSINT Suite Scripting
- 17:00 EMM End-to-End 4
- 17:00 EMM OSINT Suite Data Export and Reporting

7.3.2 Friday, 28.10.2012

- 09:15 Welcome Day 2
- Parallel Sessions:
- 09:30 EMM End-to-End 5
- 09:30 EMM OSINT Suite Use Cases
- 11:00 EMM End-to-End 6
- 11:00 EMM OSINT Suite Use Cases / Questions & Answers
- 12:15 Wrap-up & Feedback

7.4 EMM OSINT Suite – Signed License Agreements

The licensees are ordered in the sequence the license was signed.

- Belgium Police, Veurne, Belgium
- Centre for Bio security and Bio preparedness, Copenhagen, Denmark
- Ministry of Interior, Vienna, Austria

- Police Nationale DGPN, Paris, France
- Federal Judicial Police – Gent Branch, Gent, The Netherlands
- Ministry of Finance, Tax Inspection, Brussels, Belgium
- Ministry of Interior, Police, Ljubljana, Slovenia
- Police of Cyprus, Counter Terrorism Office, Nicosia, Cyprus
- Police Rotterdam Region, Rotterdam, The Netherlands
- Federal Police of Belgium, Brussels, Belgium
- VSSE (Interior Intelligence), Brussels, Belgium
- French Atomic Authority CEA, Fontenay aux Roses, France
- Danish Tax and Customs Administration, Hojbjerg, Denmark
- Finnish Tax Administration, Helsinki, Finland
- General Directorate of Customs, Prague, Czech Republic
- Customs Chamber, Opole, Poland
- Police Blekinge Region, Karlskrona, Sweden
- Italian Customs and Monopolies Agency, Rome, Italy