Strategic Pan-European Ballistics Intelligence Platform for Combating Organised Crime and Terrorism - FP7 Contract: *FP7-SEC-2007-1*

PROJECT FINAL REPORT

Grant Agreement number: 218237

Project acronym: FP7-SEC-2007-1

Project title: Strategic Pan-European ballistics Intelligence Platform for Combating Organised Crime and Terrorism

Funding Scheme: FP7

Period covered: **from** 1st November 2008 to 30th April 2011

Name, title and organisation of the scientific representative of the project's coordinator[1]:

Prof. Simeon J. Yates
Professor of Communication and Technology
Director Cultural, Communication and Computing Research Institute
Director Design Futures Centre of Industrial Collaboration
Tel: +44(0) 114 2256775

Fax: +44(0) 114 2256702
E-mail: s.yates@shu.ac.uk

Project website address: http://odyssey-project.eu/[2]

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the grant agreement

[2] The home page of the website should contain the generic European flag and the FP7 logo which are available in electronic format at the Europa website (logo of the European flag: http://europa.eu/abc/symbols/emblem/index_en.htm ; logo of the 7th FP: http://ec.europa.eu/research/fp7/index_en.cfm?pg=logos). The area of activity of the project should also be mentioned.

Contents

1 Publishable Summary Report

The ODYSSEY project undertook to research and develop a secure platform for the sharing of information about gun-crime throughout the EU. The ODYSSEY project demonstrated that data from multiple, heterogeneous sources can be combined in a high volume data repository and exercised using semantic knowledge extraction and data-mining to facilitate appropriate, fast and responsible decision making and alerts.

The ODYSSEY project's objectives were:

- The creation of European Standards for ballistics data collection, storage and sharing.
- The demonstration of a secure, interoperable platform for the management of crime information and the sharing of ballistics intelligence.
- The development of techniques for the mining of data and extraction of knowledge about gun crime across the EU.
- The exploitation of automated and semi-automated processing and analysis of crime data to generate *Red Flags* showing situational awareness through the analysis of complex data with multiple reference models.
- To adopt new and improved methods for the detection of micro- and nano-forensic information that supplement current approaches.
- To enhance mutual co-operation, security and sustainability across the EU.

1.1 Executive Summary

The objective of the Odyssey Project has been to develop a prototype intelligence platform for the secure sharing and manipulation of data about ballistic crimes. Ballistic crimes are those that involve the use of firearms and other weapons, ranging from smuggling and the supply of illegal firearms through to homicides. Although Odyssey focused on ballistics data, the concept and architecture are immediately applicable to other forensic data sets including DNA, fingerprints, mobile phone records, and explosives analysis. The techniques developed within the project for querying and manipulation could be applied to any domain that involves rich data and personal records.

The platform is built on top of a distributed architecture using message queues to link a range of back-end engines that provide the following series of components:

- Security
- Data sharing (data selection and upload, querying, storage of query plans)
- Non-relational data manipulation (semantic querying, data mining and relationship discovery)
- Support for query development (domain-specific query language, intensional support)
- An alerting component which executes queries Summary description of project context and objectives

The major outputs from the Odyssey Project were:

- A prototype system demonstrating all the key features defined in the user requirements
- A set of data standards and standards recommendation useable by LEAs and system developers for LEAs
- The identification of potential European Standards for ballistics data collection, storage and sharing.
- The demonstration of a secure, interoperable platform for the management of crime information and the sharing of ballistics intelligence.

- The development of techniques for the mining of data and extraction of knowledge about gun crime across the EU.
- Exploitation of automated and semi-automated processing and analysis of crime data to generate Red Flags showing situational awareness through the analysis of complex data with multiple reference models.
- Enhancements to mutual co-operation, security and sustainability across the EU.

1.1.1 Project Context

Globalization has been accompanied by a dramatic increase in organised and transnational crime and terrorism. It takes many forms and includes homicide, genocide, honour killings trafficking in drugs, weapons, smuggling of human beings and the laundering of the proceeds of crime. Such activities present a threat not only to citizens and their communities, due to lives being destroyed by violence, threats and intimidation, drugs and societies living in fear of organized crime; but also a global threat. These threats undermine the democratic and economic basis of societies through the investment of illegal money by international cartels, corruption, a weakening of institutions and a loss of confidence in the rule of law. Enabling cooperation across the EU is vital.

Organised crime and terrorism are inextricably linked because terrorists benefit from the financial infrastructure that organised crime provides and organised crime benefits from the financial ties terrorists build to fund their activity. The social and economic cost of crime and terrorism to the economy of the EU is extremely high and presents a major problem to economic development, growth, sustainability and social cohesion. As well as direct costs such as victims losing their livelihood, health and property there are indirect additional costs associated with investigation of crime and terrorism defeating commercial growth.

In March 2007, the Homicide Working Group at EUROPOL identified this as a fundamental issue for joint resolution across the EU and that it falls with the EU Security Agenda. The current approach fails to realise these benefits, the costs are high, risks are not tackled and security is undermined[3] . In essence it is estimated that the economic cost of organised crime across the EU is 180 Billion Euros (based on UK SOCA's statistic[4]). The challenge to security is to equip the EU with processes, procedures and platforms to deal with organised crime and terrorist threats that sustain these damaging effects on Member States economies and infrastructures. Policy makers in Security and law enforcement need to take advantage not only of innovative technological advances[5] but also the associated 'industrialisation' that comes from interoperability.

Globalisation and the relaxation of borders in the EU not only enabled people to travel freely for pleasure and commercial activity it also made it easier for criminals to travel often in possession of firearms to commit crime and terrorist acts. Currently, linking the use of a firearm used in one Member State to a crime committed in another is ineffective, highly problematic and extremely expensive. It can be done in isolated rare cases but it is not routine and does not capture the rich source of knowledge that can be extracted. Databases are localised to Member States and sometimes to Cities or Regions within Member States. The sharing of ballistics and crime information and the ability to rapidly link organised crime and terrorism is, at the moment not available and is much needed.

---

3 EU AGIS Report EUROPOL (2007); Capability of EU to Use Ballistics Information and Intelligence.

4 http://www.soca.gov.uk/assessPublications/index.html

5 Leary, R.M. and Pease, K. (2002); DNA and the Active Criminal Population. Jill Dando Institute of Crime Science. http://www.jdi.ucl.ac.uk/downloads/publications/journal_articles/PeaseLeary.pdf.

Whilst there is both political and operational commitment to share data and there is no shortage of ballistics and crime information data across the EU, there remains currently no commercially or publicly implemented technical means to do this. ODYSSEY undertook the necessary research and development to fill this gap and provide a Platform to demonstrate the effect and potential of an EU wide Platform using technical forensic data and crime information. Personal data was not be used in the prototype nor was National Security data though the developed solution presents no technical impediments to this – in fact it offers a solution to the issues of secure data exchange in a federated architecture. The Project developed a prototype secure interoperable situation awareness platform for the automated management, processing, sharing, analysis and use of ballistics data and crime information to combat organised crime and terrorism.

1.1.2 Policing context

A key aspect of the context in which the Odyssey prototype has been developed is that of existing police information systems. Internationally, there are a large number of bespoke systems including COPLINK, NABIS, HOLMES-2 and I-24/7. COPLINK is an information and knowledge management system aimed at capturing, accessing, analysing, visualising and sharing information between United States law enforcement agencies. COPLINK comprises of two components COPLINK Connect (CC) and COPLINK Detect. COPLINK Connect is designed to integrate disparate heterogeneous data sources, including legacy systems, to facilitate information sharing between police departments. COPLINK Detect tries to discover associations within police databases. It supports detectives and crime analysts in finding associations between people, vehicles, incidents and locations. The strength of an association is determined through the use of co-occurrence analysis and clustering. The system is able to search for meaningful terms in both structured (database tables) and unstructured (witness statements) data (Chen et al. 2003).

UK police forces have access to a number of independent database systems. These databases are used to record, monitor and manage offences in such areas as sex offences, gun crimes and major incident management. NABIS provides ballistic examination services, for twenty UK based police forces, through three hubs, which are based in London, Birmingham and Manchester (Sims 2010). I-24/7 has a European-wide dataset that, largely, retains information related to the individual (Interpol, 2007). A gap exists between the systems that collect, store and integrate data on ballistic crime within the EU and those which manage more general data about crimes and criminal activities. Odyssey tries to narrow this gap by combining data from a wider range of sources than existing systems do. This data was interrogated using a variety of techniques including relational queries, data mining and semantically-based searches.

1.1.3 Legal context

Both personal and crime data are very sensitive and have to be handled with care. Moving any sensitive data between jurisdictions increases the possibility that it will be compromised. Consequently a range of legislation covers data sharing within the EU. These laws and associated rules place restrictions on law enforcement agencies as they do on individuals or on businesses. Some key foundational issues are detailed in the following sections.

1.1.3.1 The Swedish Initiative

This is a statement proposing a framework for the simplification of the exchange of information and intelligence between law enforcement authorities. It was adopted in December, 2006. Nygren (2008) points out that under this initiative the rules governing the cross-border exchange of criminal information and intelligence cannot be stricter than those applying to internal data exchange. In other words cross-border data exchange should be equally as open or as closed, and meet the same security standards as within-nation exchange.

1.1.3.2 Principal of availability

The principal of availability introduces a new form of cooperation in criminal matters within the EU. Law enforcement authorities in one Member State are empowered to grant access to their information to authorities in other Member States for the purpose of prevention, detection and investigation of criminal offences. Europa (2008) states:

> "The principle subjects the exchange of law enforcement information to uniform conditions across the Union. If a law enforcement officer or Europol needs information to perform its lawful tasks, it may obtain this information, and the Member State that controls this information, is obliged to make it available for the stated purpose".

Sharing personal information or information which could be used to identify an individual has always been difficult. Under the principle of availability

> "the exchange of personal data within the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such cooperation between the Member States while fully respecting fundamental rights of individuals".

Systems such as Odyssey should be built to both encourage the use of personal data where appropriate and to ensure its security at all times.

1.1.3.3 Prüm decision

A sub set of the EU Member States (Germany, Spain, France, Luxembourg, the Netherlands, Austria and Belgium) signed the "Prüm Treaty" in the German town of Prüm on 27 May 2005 (Prüm 2010). The European Commission supported the German initiative to transform this treaty into an instrument binding on all EU Member States and the Council adopted the Prüm Decision and its implementing provisions on 23 June 2008. The Prüm Decision is described by the EU DG Home affairs as providing for:

> "the automated exchange of DNA, fingerprints, and vehicle registration data, as well other forms of police cooperation, between the 27 Member States".

1.1.3.4 Standards

The goal of the Odyssey project was to produce a prototype system that would facilitate the sharing and matching of ballistic crime data across EU member states. The above findings provide the organizational and legal context in which such a system needs to operate. From this we can identify three key barriers to effective data exchange within the EU with regard to crime data:

- There is a lack of accepted standards either formal (e.g. set by ISO or CEN) or de facto due to established practice. This includes standards for: the methods, performance and data output of ballistic matching technologies; the storage and sharing of data; and for the declaring matches between ballistics objects either through software, technology or formal process.
- There is a lack of interoperability between ballistic matching systems and police BIS
- Lack of very routine data sharing caused by limitations of the technologies (their lack of interoperability), legal frameworks, security requirements and fears and lack of knowledge or data on the value added from such exchange

1.1.4 Objectives

The ODYSSEY project undertook research and development work focused on the creation and development of a demonstrator secure platform for the sharing of information about gun-crimes throughout the EU. The ODYSSEY project demonstrated that data from multiple, heterogeneous sources can be combined in a high volume data repository and examined using semantic knowledge extraction and data-mining to facilitate appropriate, fast and responsible decision making and alerts. The initial ODYSSEY project's objectives were:

1. The identification of potential European Standards for ballistics data collection, storage and sharing.
2. The demonstration of a secure, interoperable platform for the management of crime information and the sharing of ballistics intelligence.
3. The development of techniques for the mining of data and extraction of knowledge about gun crime across the EU.
4. Exploitation of automated and semi-automated processing and analysis of crime data to generate *Red Flags* showing situational awareness through the analysis of complex data with multiple reference models.
5. To adopt new and improved methods for the detection of micro- and nano-forensic information that supplement current approaches.
6. To enhance mutual co-operation, security and sustainability across the EU.

All objectives were fully achieved apart from objective 5. During the course of the Odyssey project, changes to commercially available systems, market trends and levels of external system provider involvement radically changed the context for delivering objective 5. At the close of the project a potential solution to this, and a review of current practice had been developed by the project in co-ordination with ENFSI.

1.1.5 Targeted Objectives and Targeted Outcomes of Odyssey

Original Targeted Objectives of ODYSSEY	Actual Targeted Outcomes of ODYSSEY
1. Create European Standard: for ballistics data collection and crime information, storage and sharing to tackle organised crime and terrorism across the EU automatically combining data from disparate high volume data repositories.	Potential new EU standards for gun crime data: defined by data structures, taxonomies and ontologies in the prototype systesms. Also potential new standards for ballistics data acquisition practice developed with ENFSI.
2. Secure Interoperable Platform: Management and use of ballistics intelligence and crime information for Member States.	Automated Interoperable Platform for data sharing, analysis, situation awareness and threat monitoring. Ability for EU Member States to manage security, access and reporting using concepts of virtual organizations and circles of trust. A distributed technological infrastructure to store metadata in a semantic format for advanced querying and analysis.
3. Ability to transfer and/or access	Interoperable situation awareness enabled. Ability

technical data for cross correlation purposes. This is by securely transferring, accessing and sharing technical data.	to automate and semi-automate sharing, processing, analysis and transfer of technical data.
4. Ability to undertake data-mining and knowledge extraction of the corpus of data to tackle organised crime and terrorism across the EU to allow complex conclusions to be generated for appropriate and fast decision making.	Implemented through the use of SAS technology as well as open source solutions. This indicates that there is the possibility to extend and exploit the work of the project to other data sets for example; DNA, Fingerprints, Physical and other data.
5. Ability to exploit automated and semi-automated processing and analysis of data for generation of 'Red Flags' situation awareness by automated analysis of complex, different cultural/domain data with multiple reference models.	The ability to handle and combine real-time data feeds and historical databases for generation of 'Red Flags' situation awareness by automated analysis through semantic knowledge fusion.
6. New and improved methods for the detection of micro and nano forensic information that supplement current approaches.	Experimental and collaborative work with existing technology providers and ENFSI has identified key features of current systems. Potential best practice in system use and the potential for cross system data analysis has been identified.
7. The ability for EU Member States to manage security, access and reporting in cost effective ways.	Enable potential cost savings and efficiency gains by optimised use of data and systems. Ability to exploit automated and semi-automated processing and analysis of data for the generation of alerts ('Red Flags') to enable situation awareness.
8. Enhance mutual co-operation, security and sustainability across the EU.	Enable Member States to actively and routinely co-operate in supporting security and sustainability.
9. Business and financial aspect	Odyssey has demonstrated through the prototype the potential for a federated system to provide cost savings, *and* time savings as compared to current cross EU process.
10. High level European security cooperation	We would argue that the joint work with LEAS, ENFSI, Europol and commercial system providers has demonstrated the value of mutual co-operation across the EU in tackling organised crime and terrorism.

2 Main Scientific and technological results/foregrounds

The Odyssey project was established to demonstrate that sharing data about gun crime between authorities and jurisdictions was technically feasible and would bring operational benefits. These benefits would arise from the creation of large trans-national data sets that could be manipulated using advanced data mining techniques to reveal hitherto hidden information. During the project we developed a prototype data sharing system that met the initial objectives. Further, we identified a number of areas of Police work in both ballistics and in more general criminal work that could be standardised. The project also identified major areas of organisational, institutional and policy action that would need to be addressed to make the implementation of such systems effective.

This section describes the work undertaken to research and develop the prototype solution to the linking, presentation and analysis of cross-border gun crime data within the European Union. This domain is one where technical, policing, national and EU legal frameworks and the behaviours of police forces and criminals regularly change, sometimes dramatically within a short time span. The proposed solution described below has been developed to ensure the system can remain responsive, domain relevant and effective whilst adapting reasonably dynamically to these changes.

The objective of the Odyssey Project has been to develop a prototype intelligence platform for the secure sharing and manipulation of data about ballistic crimes. Ballistic crimes are those which involve the use of firearms and other weapons, ranging from smuggling and the supply of illegal firearms through to homicides (Akhgar, 2009). Although Odyssey focused on ballistics data, the concept and architecture are immediately applicable to other forensic data sets including DNA, fingerprints, mobile phone records, and explosives analysis. The techniques developed within the project for querying and manipulation could be applied to any domain which involves rich data and personal records.

The demonstrator platform is built on top of a distributed architecture using message queues to link a range of back-end engines that provide the following series of components:

- Security
- Data sharing (data selection and upload, querying, storage of query plans)
- Non-relational data manipulation (semantic querying, data mining and relationship discovery)
- Support for query development (domain-specific query language, intensional support)
- An alerting component which executes queries automatically

The project partners were:

- Sheffield Hallam University (United Kingdom)
- Atos Origin (Spain)
- Forensic Pathways Ltd. (United Kingdom)
- EUROPOL (Netherlands)
- XLAB (Slovenia)
- Politecnico Di Milano (Italy)
- West Midlands Police (United Kingdom)
- Royal Military Academy (Belgium)
- An Garda Siochana (Republic of Ireland)
- SAS Software Ltd. (United Kingdom)
- Direzione Centrale Anticrimine - Servizio Polizia Scientifica (Italy)
- North Yorkshire Police (United Kingdom).

The Odyssey Project also interacted with key external bodies including European Network of Forensic Science Institutes (ENFSI), European Homicide Working Group and the manufacturers of the main ballistic imaging systems in use in Europe.

Within this section we provide an overview of research and development activity of the Odyssey Project and indicate some of the key outputs. The full detail of these outputs is to be found in the Work Package Deliverable Reports, the academic and industrial publications and presentations by the Odyssey team and user workshop materials.

The Odyssey project had three main elements: an initial 'user requirements gathering' phase; an implementation phase; and a testing phase. The section details the key findings form the research element of the project and then provides an overview of the demonstrator system. The section begins with a broad review of the key findings from the user requirements research.

2.1 Key user and context research findings

2.1.1 User requirements

The requirements gathering phase was led by the partner Law Enforcement Agencies (LEAs) – not the software development or industrial partners. The LEAs were full project partners and had internal experience of gathering data on and assessing user needs. Requirements gathering events led by these partners provided the basis for identifying a set of detailed 'lay person described' user needs. The project broadly followed the Rational Unified Process (RUP) framework developed by IBM. Following RUP, user needs were translated into specific software requirements after a number of iterations and validation processes. The broad outline of these requirements was:

- All data to be held and exchanged securely
- Security by design should be a core approach
- LEAs in Member States can quickly register incidents involving ballistic items
- Potential links between ballistic, incident and intelligence data incorporated into Odyssey can be identified automatically and relevant users from Member States informed of potential links with a URN of the related records
- Firearms examiners/forensic officers can quickly examine potential links across Member State Ballistic data
- Investigating officers (OICs and SIOs) can quickly search for related incidents across Member State borders
- Analysts can quickly aggregate and assess aggregated data across member states generating intelligence products for use in prevention and disruption activity or future strategic planning
- Firearms and gun crime investigation experts can communicate with each other directly across Member State borders in a secure way
- To improve the supplier landscape for Member States through potential competition by creating less dependence upon specific ballistic analysis technologies
- An operating environment that promotes interoperability through the use of open standards (formal or de facto) and systems (such as Firetyde, XML, PKI, JMS etc.) but which maintains a robust and secure architecture that is scalable

It is not possible to stress strongly enough the centrality of secure data exchange as an expressed user need from the LEA community. The importance of this requirement was a key focus for the development of the database, architecture and interface at all points of the project. Though these

core user requirements were identified early on in the project, the economic, technological and policing context within Europe changed dramatically from the point of the grant being awarded and over the life of the project. As a result building a system that was flexible enough to address such change became an additional key user requirement. In addition to this the remit of the project included demonstration of the benefits of data-sharing, even though current legal and policing contexts might limit the actual extent to which this can be done at present.

2.1.2 Research into the broader social, technological and policy context

In order to better address these sometimes conflicting requirements and goals the project engaged in a wider review of the context of ballistic crime data collection and management around Europe. This work involved visits to a range of EU LEA's and joint work with ENFSI on understanding better the technologies on offer for the matching of ballistic items. In addition to project partners 13 EU members and nearby states (Russia and Turkey) were visited to understand available technologies and user practices. Fifteen EU member states contributed ballistic items to the joint work between the Odyssey project and ENFSI. . The policing and legal context has already been described in sections 1.1.2 and 1.1.3. From this extensive a number of key findings emerged:

- Gun crime – that is potential and actual illegal events in which firearms, ammunition and other ballistic items are involved – happens widely across the EU, though the levels and definitions of such events vary
- Many police forces and LEAs believe that criminals actively use and move firearms across the EU
- Criminals, guns and evidence travel across borders, though the levels of such use and movement are debated
- Gun crime information is collected widely across the EU, but not all the data is collected electronically, database formats, structures and data fields vary widely
- Gun crime information sharing is not routine across all member states
- Physical ballistics evidence is collected widely across the EU, and is in nearly all cases processed by experts trained in the ballistic forensics
- Roles within LEAs for the management of ballistic evidence vary widely from specialist forensic science teams to police officers trained in ballistics
- Ballistics data sharing is not routine, and the exchange of physical evidence is expensive and time consuming
- Different ballistics imaging systems exist in the market across the EU and the number and type of installations are changing (see figure 2.1)
- The different ballistics imaging systems are predominantly used for the purpose of reducing the 'search space' when matching ballistic evidence
- Matches in ballistic evidence are declared and used as evidence on the basis of direct examination by the relevant expert(s) within LEAs – not by technologies
- Gun crime prevention and detection include activity ranging from direct policing through to policy actions – at all levels good reliable data are needed
- LEAs often use multiple systems themselves to manage crime data including specific systems for ballistic data and other business information systems (BIS) to manage other crime data and business processes (see figure 2.1)
- BIS and Ballistics Systems are used for intelligence (to support on-going investigations or policy) and not for the production of evidence

- Evidential data a very small subset of intelligence data

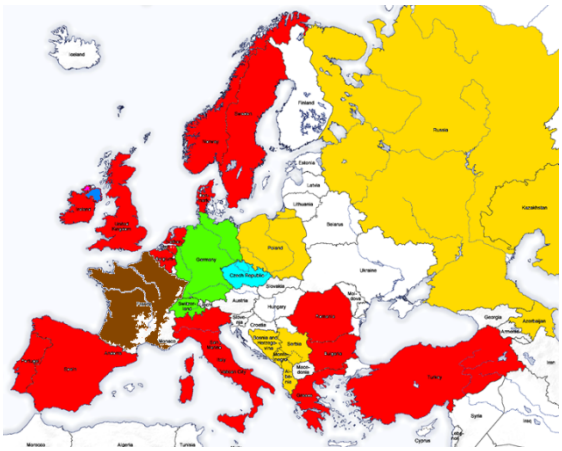


Figure 1: Variety of ballistic identification systems in use in Europe

2.1.3 Standards

The goal of the Odyssey project was to produce a prototype system that would facilitate the sharing and matching of ballistic crime data across EU member states. The above findings provide the organizational and legal context in which such a system needs to operate. From this we can identify three key barriers to effective data exchange within the EU with regard to crime data:

1. There is a lack of accepted standards either formal (e.g. set by ISO or CEN) or de facto due to established practice. This includes standards for: the methods, performance and data output of ballistic matching technologies; the storage and sharing of data; and for the declaring matches between ballistics objects either through software, technology or formal process.
2. There is a lack of interoperability between ballistic matching systems and police BIS
3. Lack of very routine data sharing caused by limitations of the technologies (their lack of interoperability), legal frameworks, security requirements and fears and lack of knowledge or data on the value added from such exchange

2.2 Key features of the prototype

The detection of pan-national ballistic crime breaks down into a number of complex problems. The first is the realisation that such crime is happening and, for the individual investigator, that their crime might be related to ones which happened across the border. The second problem is to discover the related data. Where crimes occur in different jurisdictions there may be no way in which data about them can be shared readily or easily. Only by sharing data can investigators become aware that two incidents are similar or that they may form part of a larger pattern. The final problem is to share the actual ballistic data: meta-data about bullets or guns, images taken from comparison microscopes or automated imaging systems. The Odyssey platform demonstrates that all of these problems can be addressed using a suitably complex and distributed data management application

2.2.1 Architecture

The prototype uses both local nodes and a central hub with asynchronous communication between them across a message queue. Individual components of the prototype are wrapped in Web

Services so that the platform can combine the flexibility and scalability of a modern Service-Oriented Architecture with the robustness and power of a centralised system.

A number of factors impacted upon the architecture including: the need to manipulate data which is distributed across member states; the importance of securing both data and access to it; the use of different back-ends to manipulate data; the data is likely to be both incomplete and noisy; and this is a distributed system with all of the problems which are typically found in such systems.

Data and processing have to be distributed across locations. The platform's mixture of back-ends would benefit from a single centralised data store containing records of all incidents of gun-crime from across the EU. Such a store would simplify the tracking of weapons or patterns of usage; but as noted above, the use and sharing of crime data is subject to many restrictions, some defined at European level, others set by national Governments. These regulations tend to emphasise the protection of the individual's right to privacy and generally mean that any data which might identify an individual cannot, as a matter of routine, be shared between member states. In developing software and systems for law enforcement this is usually taken to mean that data are always held locally but that individual records may be shared for specific purpose. This presents a difficulty for Odyssey that uses data mining to discover patterns within crime data. To be compliant with European regulations the platform can centralise ballistic data (guns, bullets, etc.) and some data about incidents but nothing that might be used to identify victims, witnesses or perpetrators.

Security is an important requirement for any system used by law enforcement agencies. The data that Odyssey stores and manipulates is sensitive because it often relates to on-going criminal investigations. The architecture has to balance the competing need to keep data secure and the need to share data with colleagues who, since this is a pan-European system, may work in different jurisdictions. Odyssey has a fairly standard security scheme in which users must authenticate on to the platform with an ID and a password before being given access to data and processing based on their role and location. Messages moved across the queue are encrypted using a public key infrastructure whilst the queue itself runs over a VPN.

The platform has three different data processing modules. There is a standard relational database that holds bulk data and handles queries in which target records are known or can be easily identified. There is a data mining system that is used to discover patterns within the data. Such a pattern may be a set of records which appear to be related to a particular record of interest but which do not have direct connections in the relational data, or changes to the data as when a new type of weapon enters the market and is seen to move across Europe. Finally, we have an Intensional Querying module, which through understanding the data helps investigators formulate better queries (Giacomo, 1996).

There are no standards defining the data which are gathered during investigations. Each country uses its own approach – individual organisations within the same country may even gather different data. Often the data is incomplete because officers do not have the time or expertise to enter it correctly into a computer system. Data is also incomplete because investigations are live processes. As an investigation proceeds more data is gathered and new relationships are created and existing ones modified or removed. The platform has to handle these changes and make them explicit to investigators.

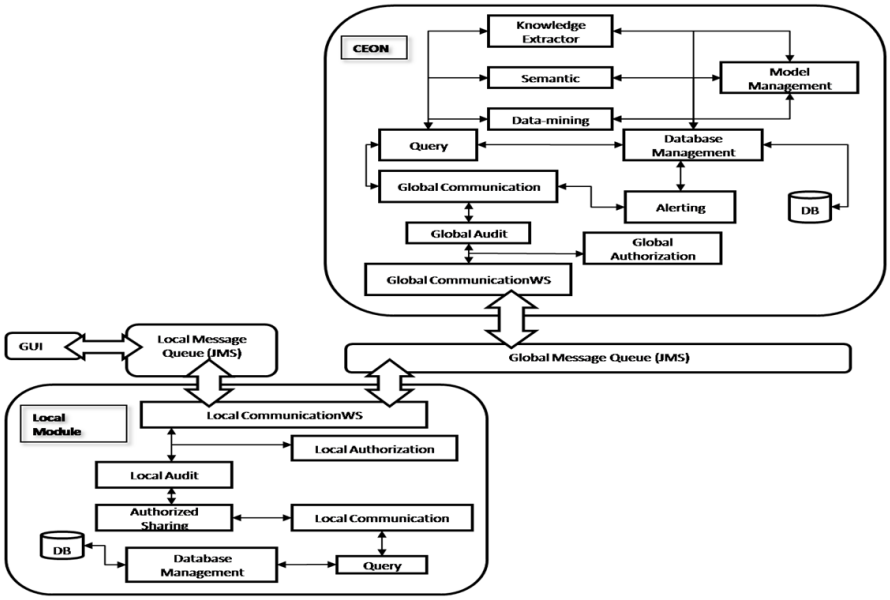


Figure 2: Architecture of the Odyssey Prototype System

The prototype has had to be designed to handle some of the more common problems of distributed systems. Processing queries can take a long time, especially when they rely on mining of large data sets. The central system has to be able to handle multiple concurrent queries which may be resident on the server for long periods. Clients cannot remain connected to the server whilst their long-running queries execute. The architecture has to be built so that clients receive responses to their earlier queries when users authenticate onto the system. This can be achieved in many ways, on the Odyssey platform it is done through the use of an asynchronous message queue.

The Odyssey platform is built from three separate modules: a local node, a Central Odyssey Node (CEON) that has richer functionality and a message queue.

2.2.1.1 Local nodes

The local node is the primary repository within the platform. The local node has a PostgreSQL relational database that holds data about ballistic items and crimes within a particular jurisdiction. The database is accessed through a local message queue and an endpoint that parses incoming requests and translates them into SQL commands which are then applied to PostgreSQL.

The local node routes “agency to CEON” and “agency to agency” communication. Using the Odyssey platform authorities are able to share secure messages including queries and their results. But its function is also an encryption of all messages, decryption and verification of all incoming messages, auditing of communication, access to local database through the IDatabaseComponent interface, interfacing with GUI components through ICommunicationComponent interface, interfacing with JMS broker, and authorizing data to be sent to CEON.

Each police force or other authority runs its own local node. When the platform is fully operational there are many local nodes running but all are independent of each other. The Odyssey desktop client gives users access to their local node but not to any of the other nodes in the system thus avoiding problems of trans-jurisdictional access to data. A node can be any size. Some may hold data for an entire nation whilst others might contain just the data for a particular area.

Using only the local node has few benefits over using existing Police information systems since any results are based on data which are likely to be in those other systems. The power of Odyssey comes from combining local and central results.

2.2.1.2 CEON

CEON, is at the heart of the platform. CEON has exactly the same queue endpoint as the local node and a PostgreSQL database which has exactly the same structure as the local one. CEON also has connections to an Intensional querying system and to a data-mining application, SAS 9.2. The platform has an experimental Semantic Web engine which tries to provide a richer querying interface through domain-derived taxonomic structures.

2.2.2 Relational Database

The main data store in the platform is a relational database developed using PostgreSQL 8.4. The database structure reflects the types of structure used in systems such as COPLINK, NABIS and by some of the databases used at EUROPOL. Most of its tables hold metadata with relatively few required to store the details of incidents and investigations. Figure 2.3 shows a fragment of the structure. The database structure is replicated at each local node. Each Local authority includes only its own data in its local node. Any data which it wishes to share with other authorities is uploaded to CEON where the same database structure appertains.

2.2.3 Manipulating the Data

The user requirements identified in the initial work of the project clearly indicated a need to move beyond simply database matching. The research and development work within the implementation phase of the project explored four distinct approaches to the manipulation of data within the system:

- Traditional database matching
- Intensional querying
- Data mining
- Semantic querying

The traditional methods were based in standard relational database searching and matching techniques. The other three methods represented attempts to solve the problems of making large and complex data easily accessible to the variety of identified potential users – from investigating officers, through forensic specialists to data analysts and policy advisors. As both an added security layer, audit tool and a method to unify search processes and their representation a 'domain-specific language' (DSL) was developed for the Odyssey system. The following sections describe the design of the three more novel methods of searching the data.

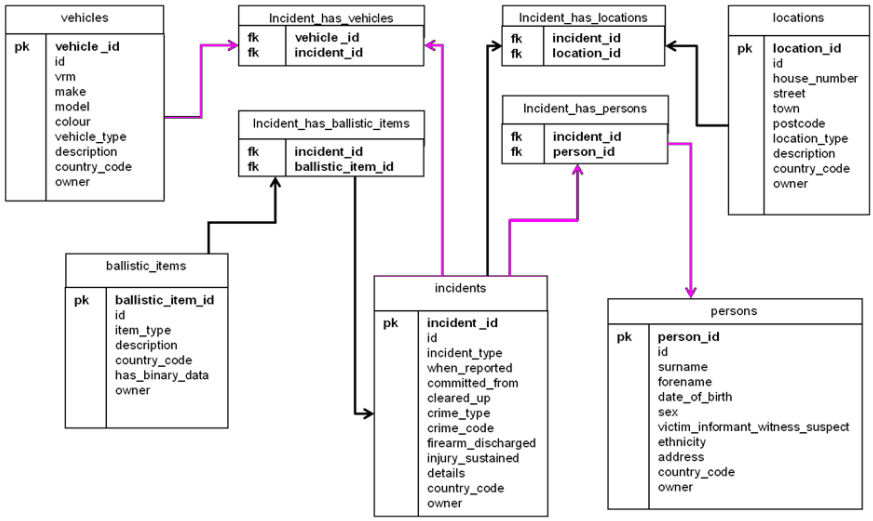


Fig. 2.3. Elements of the relational database structure

2.2.4 Intensional Querying

The application of data mining techniques to extract useful knowledge from datasets has been researched over a number of years (Nath 2006). Implementations have been tried in a number of Police information systems, notably COPLINK (Chen et al. 2004). By mining frequent patterns from repositories, it is possible to provide the investigators with partial, and often statistically-supported, results. However, such results can never be guaranteed to be completely accurate and may send investigations in the wrong direction by suggesting the wrong line of enquiry.

The Odyssey platform uses the uncertainty of data mining to give investigators implicit knowledge from the repositories and to use that knowledge to formulation more effective queries (Strohmaier et al, 2009). When a user faces a large and complex dataset for the first time they will not know its features. Frequency patterns provide a way to understand what is contained in the dataset. Summarizing the vast integrated dataset shared by different EU Police Organizations can increase the quality of results, accessing the most promising results for a given query. To this end the Intensional Querying module has been developed. We envisaged two possibilities for the use of approximate knowledge:

- The user directly queries the association rule base.
- The user queries the Odyssey repositories, but also receives an approximate answer.

In both cases the user is provided with some useful general knowledge related to the mode of investigation. In the following trivial query, expressed in Odyssey's querying DSL:

```
WHAT ABOUT Incident Person WHERE country_of_crime = 'UK' AND gender='m' WITH CONFIDENCE 0.9
(
```

The statement triggers the intensional knowledge system to return any information about the listed elements given the defined conditions. Thus every association rule containing:

- (at least) attributes from the relations translated from the keywords in the WHAT ABOUT list (for example Incident, Person)
- in which elements satisfy the conditions (for example country_of_crime = 'UK' AND gender = 'm')
- having confidence more or equal than the stated value (for example 0.9)

The results are sent back to the intensional system for further processing such as ordering. The completed result set is returned to the client where it acts as a prompt, or set of prompts, to the user to help them either refine or widen their search criteria.

2.2.5 Data Mining

The CEON component includes a full SAS data-mining system which is used to manage data uploads through its excellent GUI tools and to mine the repository looking for patterns and hidden structures. The data-mining and knowledge extraction modules need to pre-process the database data in order to extract information for its later use. In particular, SAS data-mining solution requires for a de-normalised version of the data (Wilson et al, 2010). Processes to load any data which has changed into SAS and add it to the de-normalised structure are triggered periodically to keep it up-to-date. Mining queries may then be re-executed. The reason that Odyssey has a central database is so that it can mine data. The benefit of centralising and sharing is that much richer results can be obtained. When a data mining query discovers data it actually returns only record IDs. The middleware sends these IDs to the CEON instance of Postgres where they are used in SQL SELECT statements to retrieve complete records. These records are returned to the user who initiated the query.

2.2.6 Semantic Querying

The final component, which is available to users, is a Semantic engine. One of the first acts of the Odyssey project was to define the taxonomy of ballistic items and ballistic crimes. Inputs to, and outputs from, the platform must be structured according to this taxonomy.

Organisations using local nodes are able to share data by uploading it into CEON. Typically they will upload a subset of their local database composed of records that they have permission to share. Most of the data held in Odyssey can be shared without encountering problems of privacy or confidentiality. For example, the details of a used cartridge case are not likely to be confidential. Data about crimes and possible crimes are more sensitive since from these it might be possible to identify people. Where data is sensitive in this way the platform lets authorities share those columns which will not conflict with data management legislation.

The kinds of queries, which investigators ask, are conceptually rich and include a lot of uncertainty (De Bruin et al. 2006). In Odyssey these queries are handled using a semantic engine that runs at CEON. Queries are converted into SPARQL and applied to the data through a Jena engine. Both the semantic engine and SAS are used to automate and simplify the process of discovering similar data to that which is being investigated. This gives detectives the opportunity to find hidden relationships within trans-national datasets that they would otherwise never find.

The semantic engine lets users build queries that are dependent on their role. A crime analyst may want to ask different questions to those which a detective asks - they may be more strategic or intelligence-led, whilst the detective is focussed on operational matters. Such roles are not static. The same user may sometimes require intelligence data and at other times require operational information. Vallet et al, (2007) note that

> "users may have stable and recurrent overall preferences, not all of their interests are relevant all the time. Instead, usually only a subset is active at a given situation, and the rest can be considered as noise preferences"

The platform has to take into account the changing context within which a user queries the system. For a broader view complex context in which such semantic solutions need to operate.

Both semantic technology and data mining are aimed at efficient retrieval of desired information. These technologies work on the raw data with the goal of retrieving useful information as an end result that can provide the baseline knowledge needed. But each of these technologies pursues the same goal using different approaches. Semantic modelling techniques focus on representing the raw data using formal structures. Information retrieval from the formalized structure becomes very efficient by as they enable intelligent reasoning and inferencing. On the other hand, data mining techniques rely on the use of efficient algorithms to retrieve useful knowledge from the data as shown in the figure 2.4.

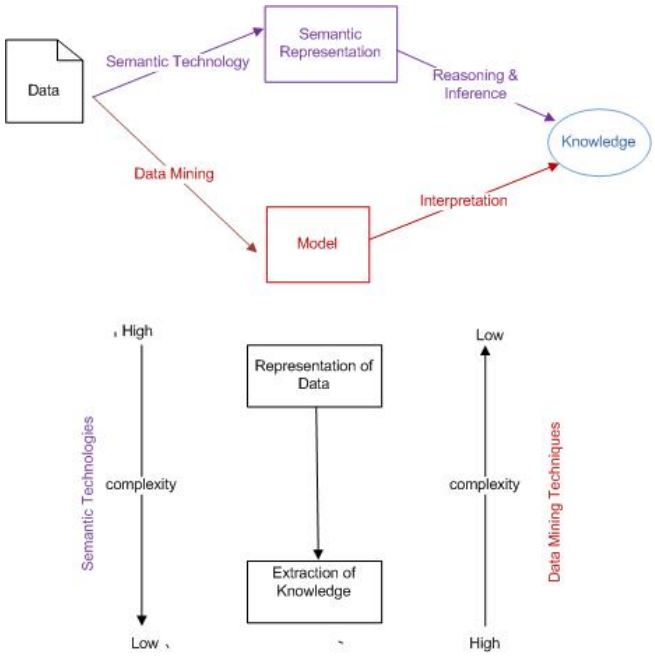


Figure 3: Semantic search versus data mining

As a result semantic technology pushes the level of complexity high on the efficient representation of data whereas data mining techniques impose high complexity on the efficiency of the extraction algorithms. So, a balance can be maintained between the two extremes and it is possible to get the best of both technologies. In context of Odyssey given the previously identified user requirements and ever changing context of criminal investigation processes, it was essential to combine both data mining and semantic approaches.

2.2.7 Query Language

Users of the Odyssey system will be experts in the gathering and analysis of complex, incomplete data. Detectives and crime analysts or other civilian support staff are experts in the understanding of crimes through the use of rich data such as statements or observations (Smith & Tilley, 2005). This intellectually complex work requires a clear cognitive focus and well-honed skills. The Odyssey platform is a very complex piece of software. Users cannot be expected to know that their queries are being applied to different back-ends or what data structures are used within the system. Indeed their use of the platform should, wherever possible, be natural so that the system supports and enhances their usual working practices.

A domain-specific language (DSL) is an artificial computer language which is used to describe solutions to constrained problems. A DSL provides a natural and effective interface between a complex system and its users,(Fowler & Parsons, 2010) which can be more expressive than operations constructed purely through a GUI. DSLs express complexity at a particular abstraction tailored to both current and future needs (Yu, 2008). A DSL lets non-technical people understand the overall design of a platform and interact with it, using an understandable notation that reflects their particular perspective (Bonino et al. 2004).

The DSL that was created is called the Odyssey Semantic Language (OSL). It supports the modelling of active crime investigations by operational detectives and facilitates the linking of generic crime features to ballistic data. Its innovative features are associating data retrieval techniques with data-mining results and encapsulating multiple services. Moreover, the language facilitates modelling of investigation processes and is an integral part in the platform's security.

2.2.7.1 Defining the DSL

OSL is a formal language specified by a context-free grammar. The OSL grammar was structured to make use of tokens taken from the English language in such way that the resulting constructions, that is, those sentences considered valid by the grammar, resemble the natural language of investigators so as to facilitate their construction and interpretation, (Jopek et al, 2010).

The grammar is defined in the Extended Backus-Naur Form within the ANTLR framework, a language recognition tool that simplifies the construction of a parser and lexical analyzer pair from the grammar definition, as well as allowing for additional embedded code - in this case in Java. This simplifies the creation of a translation into the languages needed for the subsystem modules which are mainly SQL.

The language has relatively few keywords. Most keywords actually occur inside meaningful phrases as shown below:

GET CHARACTERISTICS returns a taxonomic structure: GET CHARACTERISTICS Person returns all the fields that describe a person (gender, ethnicity, age, etc.)

IS IT TRUE THAT returns "Yes" if the condition is true otherwise "No". For instance IS IT TRUE THAT Vehicle HAS PROPERTY VehicleMake WITH VALUE ‘Saab’

SHOW STATISTICS gives simple statistical information such as average value, standard deviance and variance about records matching certain criteria. For example SHOW STATISTICS ON PersonEthnicity WITH VALUE 'white'.

SHOW SIMILARITIES BETWEEN: SHOW SIMILARITIES BETWEEN Person WITH VALUE 1 AND 13.

SHOW QUERY / SHOW ALL declare a simple retrieval from database. The difference between them is that SHOW QUERY creates normal joins between tables whereas SHOW ALL does a full outer join between tables.

WHAT ABOUT executes an intensional query: WHAT ABOUT Person Vehicle WHERE VehicleMake = 'Ford'

SHOW SIMILAR returns all records that are share the value of at least the given number of columns with the given instance: SHOW SIMILAR Person WITH VALUE 1 HAVING 4 EQUAL COLUMNS

CONFIDENCE: the value specified affects the number of results returned to the user. The higher the confidence the smaller the returned result set. For example WHAT ABOUT Person WHERE ethnicity = 'white' WITH CONFIDENCE 0.5.

The example below presents a query expressed in Odyssey Semantic Language (OSL) that retrieves firearms with a twenty-two calibre:

```
QUERY firearm WHERE calibre HAS VALUE 0.22
```

Typically requests into the system begin with QUERY. This term was chosen because there are so many possible terms (SEARCH, GET, FIND) that we needed one which was neutral and meaningful. OSL is used to upload data, share it and modify it which is why all operations need to begin with a keyword which identifies the operation (QUERY, UPLOAD, MODIFY, ALLOW).

In the example, firearm is used to identify the database table that is going to be searched. Users are never told that this is a table. They interact with a set of objects which come from their domain, from detective work. These include firearm, cartridge-case, bullet and incident. All queries are assumed

to return a set of records which are presented to users as domain-level objects rather than as records, although that set may be empty or may contain just a single item.

Queries are retrieved from the message queues by a layer of middleware that parses the OSL and converts it into one of SQL, SPARQL, SAS' ProcSQL or into an intensional query. The choice of backend language depends upon the nature of the query. Queries for the PostgreSQL database begin with the keyword query, those for the SAS data mining system with SIMILAR and those for intensional with WHAT ABOUT.

The conversion from OSL into a query language gives heavily optimised queries with the minimum effort from users. The following example shows how a simple statement becomes a query across three tables with a series of optimised joins.

```
QUERY ballistic incident WHERE weapon_manufacturer HAS VALUE Sig Sauer AND victim_gender HAS
VALUE female

SELECT * FROM odyssey.ballistic_incident

LEFT JOIN ballistic_incident_has_recovered_firearm ON
(ballistic_incident_has_recovered_firearm.recovered_firearm_oid
= ballistic_incident.oid)
LEFT JOIN ballistic_incident_has_recovered_firearm ON
(ballistic_incident_has_recovered_firearm.recovered_firearm_oid
= recovered_firearm.oid)
LEFT JOIN ballistic_incident_has_case ON
(ballistic_incident_has_case.ballistic_incident_case_oid =
ballistic_incident.oid)
LEFT JOIN ballistic_incident_has_case ON
(ballistic_incident_has_case.ballistic_incident_case_oid =
case.oid)

WHERE case.gender_of_victim = "female"
AND recovered_firearm.manufacturer = "Sig Sauer";
```

2.2.8 Alerting

A key element of the user requirements was an alerting component. The alerting component monitors a set of queries defined by the user. These might include an alert should any newly input evidence become linked to on-going investigations. For example should a vehicle, person or ballistic item be introduced to the database (local or CEON) which links relationally to a current item of interest. Alternatively should the results of any other stored query defined in the Odyssey DSL change due to changes in data within the local or CEON repositories an alert can be raised. The alert will go to those LEA end users who instantiated the query or indicated an interest in the item. The alert provides them with the details of the query who's results have changed. As a minimum the alert provides details of the URNs relevant to the items and the member states to which they belong. This provides a minimum data exchange in order for LEA officers to determine if further data exchange is needed, or if a new line of enquiry has been identified.

2.2.9 User interface – hiding the DSL

Users have been at the core of the Odyssey project, but which users? In undertaking the broader work on user needs, user context, user practices and available technologies the project identified a wide range of potential and actual users of ballistic identification systems and crime BIS - as noted above these users range from investigating officers, through forensic specialists to data analysts and policy advisors. In many cases user expertise will be in policing, forensic science and only in a

few cases information system use, database querying or data analysis. In our research we did note the extensive use of graphical representations of the relationships between data items. This may have been for use by specific groups of experts or for communication between staff with differing roles. Often actual or potential links between crimes, events, items of evidence, people and locations were presented in networked graphs. This may be supported by specific tools, such as those provided by i2 (which merged in 2009 with the software provider of COPLINK), or may be 'drawn by hand' in standard vector graphic tools. Such network diagrams have become a standard form of visualization within this law enforcement domain. The Odyssey project therefore sought to use this form of representation within the interface to the underlying data, and as a visual method for execution of operations and queries within the system.

The Odyssey platform returns results as sets of linked objects. These are displayed in a desktop application. The user is able to see graphs of objects and, by manipulating their properties, can build new queries easily and quickly. Query plans can be saved so that the query can be re-executed later. These plans are simple OSL statements which can be shared between users, for example on email.

The GUI does not present a differentiation between queries intended for the semantic, relational or mining back-ends. Queries are executed across all of the querying systems unless the user edits the OSL to prevent this. Results from all of the back-end systems are integrated into a single graph.

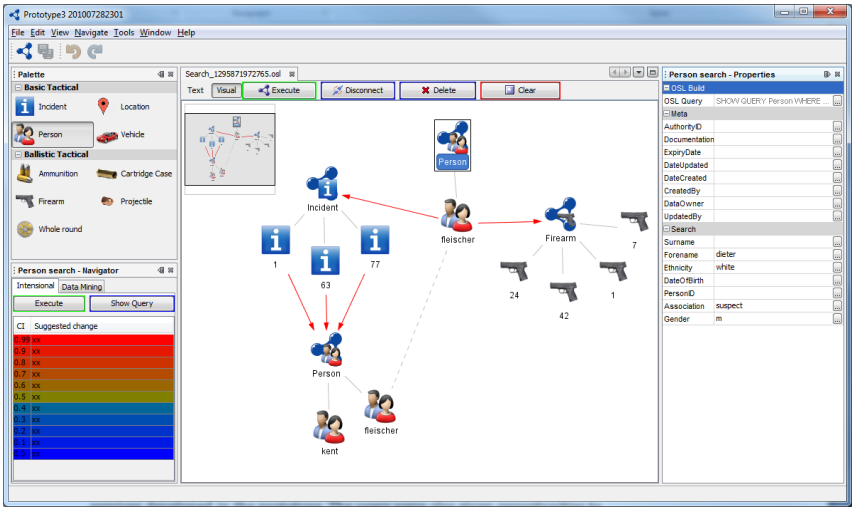


Figure 4: The GUI applying the networked graph representation

Figure 2.5 shows how the graphical user interface of the Odyssey platform facilitates search and browsing across the entire crime and ballistic dataset. It takes the full advantage of inductive and deductive approaches so that the end-user can inductively find relevant information and deductively identify values while browsing and narrowing down the possibilities based on the information presented. The interface enables building advanced queries while hiding the complexity of the underlying data structures from the user.

The output of the intensional module is shown on the left of figure 2.5. Different colours are used to indicate the strength of association which the module has discovered. The user may choose to modify their query using the changes which are suggested here. This is done simply by selecting a suggestion - the GUI automatically re-writes the query for the user.

Presenting result graphs and using them to build new queries is an established GUI technique. The Odyssey project validated the approach through extensive testing with users. The project's validation process included a demonstration of the applications and services developed in the prototype. Users were also given opportunities to interact with the prototype. This allowed the Consortium to review the high level objective of the Odyssey platform, whilst evaluating the

Stakeholders continued expectations and needs. In line with the adapted research method the lesson learned during the validation process was elaborated into new set of requirements for the third validation cycle.

2.3 Implementing the prototype

2.3.1 User requirements

The user community recognised that the project had to be mindful of the current legal and technological constraints in designing a data-sharing application. However this does not mean that the project was to be bound by those constraints in looking beyond state of the art. That said, it is important to note that the requirements work within the proposed European legal framework concerning information sharing and data protection and seek to prevent development of any anti-competitive practises by setting open standards that can be utilised by any current or future supplier.

The Odyssey system is independent and self-contained; it is not reliant on any of the current ballistics technologies on the market but seeks to interoperate with all of them. Any data held within the Odyssey platform remains distinct and self-contained ensuring maximum local control remains with Member State owners of the data.

The User Community identified that, for the purposes of this project, the highest-level requirements will need to satisfy the following conditions:

- All third-party personal information will be excluded from the scope of this project (e.g. suspects, offenders, victims and witnesses). Personal details of Member State agency staff may be included for reference purposes.

- Optimisation of central and local costs of hardware, software, development, use, administration and maintenance (physically and for configuration of the system and administration of data and users)

- Development of an architecture that ensures the ability for fast time results where necessary for developing investigations. It is accepted that large scale analysis of data may take longer but this type of use of Odyssey will usually be for strategic rather than immediate operational purposes.

- Optimised information security through minimisation of data and information transfers between central and/or local information repositories as well as substantive support for reactive and proactive audit of data and user interaction where required.

- Furtherance of the EU's ambitions to share critical intelligence on serious and organised crime

The information contained within Odyssey is managed and protected by a competent authority and investigative links will be reported to Member States through unique reference numbers. Member States communicate about the URN link and make their own intelligence sharing arrangements, thereby retaining overall control of the actual information sharing process.

Wherever possible, relevant tactical or situational intelligence and ballistics data is automatically incorporated into the relevant Member State's repository within the Odyssey system. Odyssey users can enter data directly wherever automated processes are not possible however it is recognised

that the double-keying of information is both time-consuming and increases the likelihood of reduced data quality through keying errors made by users re-keying information.

The system can be used to identify trends of weapon use across the European Union and the proliferation of specific types of weaponry and ammunition through its integration of a number of forms of data mining. The Odyssey system responds to user-defined searches and develops an intelligent, automated search based on them. Odyssey remembers searches and identifies links which may emerge sometime after the original request.

2.3.2 Process model

During the project we recognised that handling of information and investigations is done in many different ways. It became clear that there are pieces of information and processes which ought to be collected or followed whenever possible. These were gathered into a single unified process model.

The Odyssey process model consists of a step-by-step workflow in which ballistics evidence and associated information about crimes involving firearms is collected, stored and processed. It is recognised that different procedures and policies are andbe in place in different countries across the European Union. This workflow is aimed at providing a high level overview of the process and it is recognised that there are and will be variations between countries.

This workflow model assumes that every country uses a ballistics analysis system. It is recognised that different countries are using different ballistics analysis systems such as Evofinder, Arsenal, Balscan, Poisk, Tias and IBISTrax. All points that refer to automated ballistics analysis systems are meant as a general overview of the process allowing for the individual differences between the systems. The process model was validated by the user community within the project and disseminated more widely. It received a favourable reception and will be further enhanced at a later stage.

2.3.3 System architecture

Because Odyssey would connect many authorities in many different geographical locations, we decided to use a service-oriented architecture (SOA). We selected the specific technologies by focusing on: the robustness of the implementation; the existence of push mechanisms; and security. Our selection of technology aims for loose coupling of services so that the developers could use the most suitable technologies for the problem they are solving. The following figure shows a high-level schematic of the Odyssey system. We have one or more local authorities that can have one or more GUI applications connected to the platform and at least one database. All local authorities are connected to the Central Odyssey Node, CEON, using the Java Message Server protocol. On CEON's side all the processing and modelling using the gathered data is done.

2.3.4 Local audit component

The local audit component writes all local audit logs. The local audit component makes use of the audit component in the interface with the GUI which guarantees that it is not possible to make a function call to any of the interface functions without an audit trace.

2.3.5 Local communication component

The local communication component is a local component which implements the logic that is needed at the local authority. It loads objects necessary for communication with JMS broker, auditing, database, encryption, decryption, etc.

2.3.6 Authorized sharing component

The authorized sharing component modifies the data set sent to CEON in a way that only authorized data can be sent. In this way, the local authority makes sure that sensitive fields are

stored only in the local database. Once data is already at CEON, a change in the authorized sharing component will not affect stored data, only the new inserts. There is an option to remove the data already on CEON, but this is not managed by the authorized sharing component. Administrators have an option to setup different limitations according to these sharing policies:

- user data sharing policy: which information can this particular user share
- local data sharing policy: which information can this local authority share
- data depersonalization policy: which attributes can be shared

Authorized sharing component takes into account the aforementioned policies and strips the incoming stream of data of all information that is not allowed to be shared.

2.3.7 Global Audit Component

The global audit component writes all central audit logs. Global audit component implements an interface with listener components which guarantees that it is not possible to process any messages without an audit trace.

2.3.8 Global communication component

The global communication component is a central component in this design. Its functionality is to implement the logic that is needed for processing messages on CEON.

2.3.9 Global authorization component

The global authorization component is responsible for authentication of all users connected into the Odyssey system (this includes local modules), and for the access authorization to data for these users. All queries and inserts must be approved by this component.

2.3.10 Query component

Query component translates OSL queries into the appropriate format for the corresponding component, and ensures that translated query is forwarded that component, which in turn does the actual processing of the query. In case of an SQL query, this means a database management component. The use of OSL as an intermediate language improves the security of the database against SQL injection-attacks.

2.3.11 Database management component

Database management component performs all “raw” SQL queries in the relational database.

2.3.12 Semantic component

The semantic component is responsible for running SPARQL queries against the semantic database. We currently use the framework Jena for the taxonomy management, but we have shown that using an ordinary reasoning engine on a small data set had an unacceptable time response. The component is currently used for taxonomy management.

2.3.13 Data-mining component

The data mining component is responsible for generating data mining queries and executing them in SAS data mining software.

2.3.14 Alert generation component

The alert generation component periodically scans a list of stored queries and notifies the subscribed user if any results are finally found.

2.3.15 Knowledge extraction component

Knowledge extraction from datasets can be very useful for the users to obtain information and implicit knowledge in the repositories, and to be more effective during the query formulation process. Given an SQL query, the output of this component is a set of association rules. For a normal database query of the form "*Retrieve all the incidents involving a Ford vehicle", we can obtain a rule such as "Fire gun deaths* involving a Ford vehicle mostly involved 'Asian' ethnics". These rules have a confidence value that can be used to evaluate their importance.

2.3.16 Model management component

The component manages all the models that are result of the artificial intelligence components in the Odyssey. This component manages metadata of each of these models thus providing consistency for querying, history of models and can even be used for authorization purposes. The component is best described with an example: the data-mining component is used to build a regression tree from the Odyssey database. The model management component stores the tree and add the following attributes: time of creation, the datasets used, the properties and version of the regression tree induction algorithm. When a query, which can utilize this regression tree, is issued, the metadata is also presented, so we know which version of the tree returns the result.

2.3.17 System security

The Security Module is the ODYSSEY component responsible for providing security and access control services for guaranteeing that all exchanges and access of information are protected in a proper way. In order to secure all Simple Object Access Protocol (SOAP) messages sent over JMS, OASIS Web Services Security (WS-Security) standards have been adopted in conjunction with a Public Key Infrastructure (PKI) model. The ODYSSEY security layer is based on Apache's WSS4J, a Java implementation of the WS-Security specification that is used to sign and encrypt all messages exchanged in the ODYSSEY platform providing security confidentiality, integrity, authentication, and non-repudiation in a transparent way from the application point of view.

Two different approaches can be followed to protect WS architectures, apply security at transport and/or at message level. Transport layer security represents an approach where the underlying operating system or application servers are used to handle security features. Whereas, message layer security represents an approach where all the information related to security is encapsulated in the message. In ODYSSEY we have selected this second approach since it offers several but the most important one is the increase of flexibility. Parts of the message, instead of the entire message, can be signed or encrypted. This means that intermediaries can view the parts of the message that are intended for them. This feature adds the support for auditing, where intermediaries can add their own headers to the message and sign them for the purpose of audit logging. Nevertheless, a VPN has been set up in ODYSSEY protecting also the messages at network level.

Traditional security technologies are not sufficient for Web services security because of the need to secure data and components on a more granular scale. Because Web services use message-based technologies for complex transactions across multiple domains, traditional security processes fall short. A Web-service message can traverse several intermediaries before it reaches its final destination. Therefore, the need for sophisticated message-level security becomes a high priority and is not addressed by existing security technologies. To deal with the threats described above, we have selected WS Security standards (WS-Security) that describe enhancements to protect

SOAP messages through XML digital signature, confidentiality through XML encryption, and credential propagation through security tokens.

For controlling the access to the data, a Role Based Access Controls mechanism has been incorporated in the Security Module at both, Local Authority and CEON level, letting components or the GUI check the user privileges before authorize a user operation.

Additionally, the Security Module also includes a multi-factor authentication mechanism based on the ownership of a key storage where the users will be asked first to have a valid Odyssey key storage, secondly the password to open this key storage and finally, the password to access to the private key that will be used to decrypt and sign messages.

Web Services Security (WS-Security) standards have been adopted in conjunction with a Public Key Infrastructure model as reference architecture for the Security Module. ODYSSEY security layer is based on Apache's WSS4J, a Java implementation of the WS-Security specification that is used to sign and encrypt all messages exchanged in the ODYSSEY platform providing security confidentiality, integrity, authentication, and non-repudiation in a transparent way from the application point of view.

2.3.18 Data manipulation and visualisation

The aggregation module is in charge of collecting the information produced by the data mining module of the platform, and presenting it to the user.

The module has two sub-components:

- The information presentation module: responsible for connecting the Odyssey platform with the user and returning results.

- The information aggregation module: in charge of connecting the Odyssey platform with the data mining software.

The SAS-Odyssey integration is based on Web Services (WS), as we exposed a generic SAS procedure through a WS. The general idea is to expose SAS procedures through a WS to make them accessible for the Odyssey system.

The Odyssey GUI makes use of the output provided by SAS in terms of correlation or sorting results by their relevance. The SAS tools build scoring models; to do that they define the likelihood of two elements to be similar. In the GUI, the graphs are annotated with the data mining results. This could be used in the GUI as clustering method to define whether two locations are near to each other or not, depending on the data within the system. These models can be used for data input quality assurance process or looking for inconsistencies and anomalies.

Additionally, the Odyssey GUI provides users with a comprehensive query and messaging capabilities, including all the functionalities required to interact with the Odyssey platform, while hiding the technicalities of the Odyssey architecture.

2.3.19 Data structures

2.3.19.1 Taxonomy

Within this section we describe the Odyssey Taxonomy. As the taxonomy itself is too large for effective presentation here we refer readers to other public outputs of the project in which it is detailed.

Our work continues with the description of the actual data available to the Consortium and various approaches of utilizing this data to extract meaningful results, as requested in T4.2. Technologically,

we do not rely on the ontology reasoning, but rather employ novel hybrid approaches that utilize the operator and/or taxonomy knowledge to extract relevant rules.

The specification of the ballistic standard is closely related to the NABIS and FireTyDe specifications. Work on the Odyssey extensions produced additional concepts in the current Odyssey Taxonomy. The current work regarding the knowledge application, knowledge guidance of the search for new potential knowledge, hidden in the data is thus using the concepts in the current Odyssey Taxonomy. The extensibility of the latter is also used in the algorithms for pattern-mining within the data.

The taxonomy represents a classification of all the concepts that appear in the scope of knowledge which our application should cover (e.g. crime data including firearm identity classification). The Odyssey taxonomy is designed to support future implementations and expansions of the Odyssey ontology.

2.3.19.2 A high-level description of the Odyssey Taxonomy

The resulting Taxonomy has the four top elements:

- **Event:** This node includes all the information regarding some incident, incident description, ballistics information, recovery, etc. This node is the most important node in the whole taxonomy.
- **Document:** The documentation, as such, should be unified and used when documenting an event – this node could also be sub-node of the Event, but as it is of utmost importance to define and unify the concepts of the documentation on the EU level, hence, we decided to make it one of the top-level nodes.
- **Movement:** The reasoning behind making this node one of the top-level nodes is the importance of physical movement of the ballistics items. The documentation about the ballistic items movements should also be unified on the EU level – the reason for making this node as one of the top-level nodes.
- **Value Partition:** This node serves as auxiliary node, with all the currently known concepts that should serve as types, values or be otherwise connected to the concepts in other nodes. The approach was to avoid the actual instances and rather employ the Value Partition pattern and use restrictions thus enabling simple future additions (specializations) of the concepts in this sub-tree.

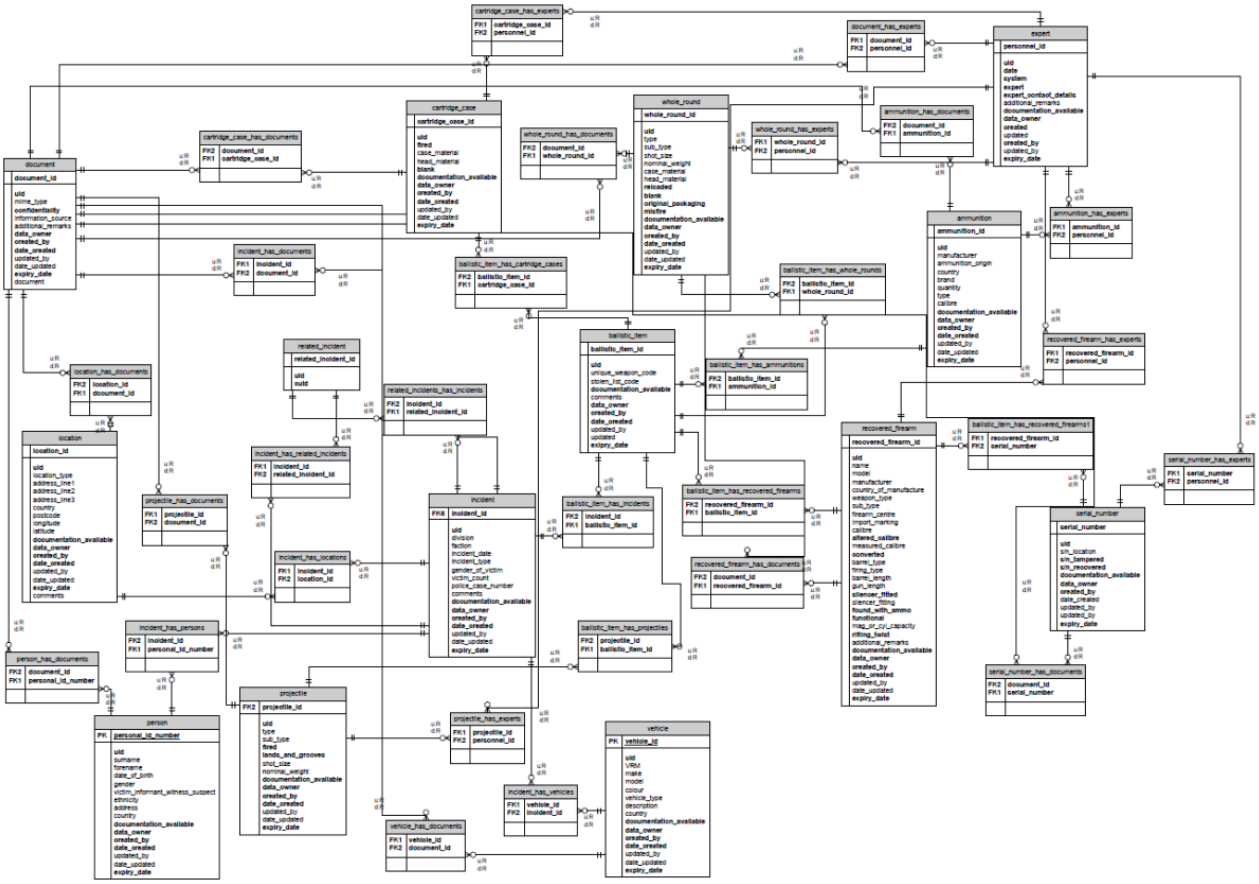
2.3.20 Database

The Odyssey Database is implemented using PostgreSQL database, which does not support export of the data into the flat table. It is worth mentioning that use of the OSL to get the descriptions of the needed attributes does not fulfil our needs completely, as it performs left outer joins over the tables and their primary and foreign keys.

We thus used a simple method, based on our knowledge of the data structure. We can see that the main table within the structure is Incident, thus it is the starting point – all incidents are always in the flat table. The associated data may exist or not – in the case where the associated tables have appropriate records we include them, otherwise we just write common “?” sign, denoting the missing data. A special case is when the associated table has more records for one record in the primary table. In this case, we replicate the record in the primary table and concatenate all records from the associated table, respectively.

The end result is a flat table, containing all attributes from the database and all records from the Incident table and associated tables.

The technical details of the implementation are not within the scope of this document. It should suffice to explain that the module is written in Java and relies heavily on reflection – as such, it is capable to flatten Odyssey Database even if the attributes completely change.

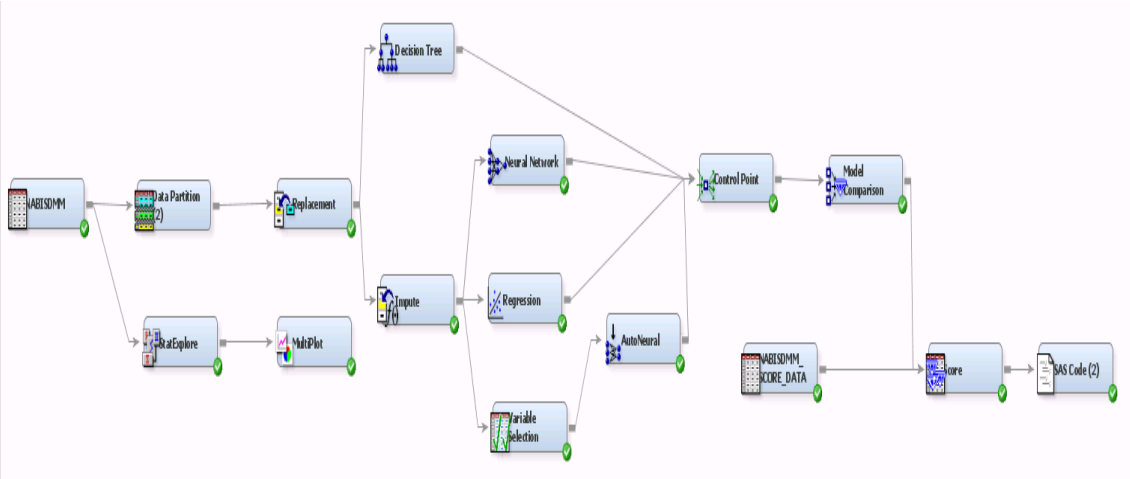


2.3.21 Mining

2.3.21.1 Using SAS

The SAS-Odyssey integration is based on WS that we exposed a generic SAS procedure through a WS. The general idea is to expose SAS procedures through a WS to make them accessible for the Odyssey system allowing in this way to load and extract result from the SAS software.

We used SAS Enterprise Miner to create three models that could be used to identify a potential association from the Ammunition Manufacturer, Gun Type or Incident Type. Using the NABIS Data Mining Mart, created using the SAS Integration Studio, an Enterprise Miner process flow was created.



After exploring the data using SAS StatExplore and MultiPlot, the NABIS Data Mining Mart was then partitioned in to Training, Validation and Test data sets. A replacement node was then added to replace any missing values (with "unknown") within the data set. A decision tree node was then added to the process flow to predict the target variable. An Impute node was then added so that the number of unknown values didn't weaken the Regression and Neural Network models. The results from the different data mining techniques are then filtered through a control point before they are passed to the model comparison node. The model comparison node was then used to automatically select the best model. This model was then used to score the dataset.

The final scored data set contains the Incident Number, Ballistic Item Number, a predicted classification and probability.

2.3.21.2 Using intentional querying

The application of data mining techniques to extract useful knowledge from datasets has been widely applied in the literature. By mining frequent patterns from repositories, we provide the users with partial, and often approximate, information on the dataset's content. A user may be interested in obtaining a quick approximate answer to a generic query, for example, "Find the most relevant information about crimes in Spain".

This kind of queries is helpful especially in wide-range analyses involving a huge amount of data and to discover frequent correlations of values, which can be used later to write more specific queries. At this stage the user will be mainly interested in the confidence associated to the answers which is defined as $\text{confidence}(X \Rightarrow Y) = \text{support}(X\ UY)/\text{support}(X)$, where X and Y are sets of values appearing in the dataset (itemsets) and $\text{support}(X)$ is defined as the proportion of records in the dataset which contain the itemset X.

The WHAT ABOUT statement has been developed to integrate with OSL. Using this statement, a user would direct his/her query *only* towards the intensional repository of previously mined association rules.

WHAT ABOUT Incident Person

list of keywords from the ontology/taxonomy to be translated into real system values (relations in the real database)

WHERE country_of_crime = 'UK' AND gender = 'm'

conditions on keywords representing attributes from the relations at the ABOUT level with AND, OR connectors

WITH CONFIDENCE 0.9

lower bound value to be considered in rules confidence

The statement will trigger the intensional knowledge system to return any information regarding the listed elements given the conditions, and thus every association rule containing:

- (at least) attributes from the relations translated from the keywords in the WHAT ABOUT list (for example Incident, Person)
- in which elements satisfy the conditions (for example country_of_crime = 'UK' AND gender = 'm')
- having confidence more or equal than the stated value (for example 0.9)

In order to get back any result from the intensional repository, the WHAT ABOUT statement needs to be processed by the OSL interpreter, to have keywords translated into SQL relations and attributes of the database, then it can be sent to the intensional system to be processed.

Alternatively, the user queries the regular Odyssey repositories, but also receives an approximate answer. In this scenario the Odyssey user composes an SQL query but he/she will receive both the traditional, extensional answer, and when possible, the intensional answer. The IQ4CSI module parses the input SQL query and rewrites it in order to be applied to the mined association rules.

Given an SQL query, the output of the intensional module will be a set of association rules that can be represented either in a relational format, or as an XML document, or in a more intuitive/graphical format. In a textual document, as this document is, the result of a query is shown as a set of implications for readability reasons. The mined association rules are stored in a relational database with the following schema:

- nodes (node_id, table, attribute, value)
- rules (rule_id, support, confidence, num_antec, num_cons)
- antec_cons (ant_cons_id, node_id, rule_id, ant_cons)

2.3.22 Semantic querying

2.3.22.1 Classic Semantic Reasoning

During our experiments with the incorporation of knowledge into the induction of new knowledge from data, we built ontology from the smaller parts of the taxonomy. Within these experiments we introduced instances into the ontology, based on the Odyssey Database. The properties of the ontology were rather simple, and mimicked relationships in the data.

Querying of the so-populated ontology using SPARQL took a long time – even for some of the simpler queries. We then performed a number of optimizations of the ontology and the instances and improved the querying time. Still, given the expected number of examples in the final Odyssey Database and the actual data management overhead, we decided to stop the activities in the area of ABox-level reasoning and focus on supporting of the machine learning with additional knowledge and guidance.

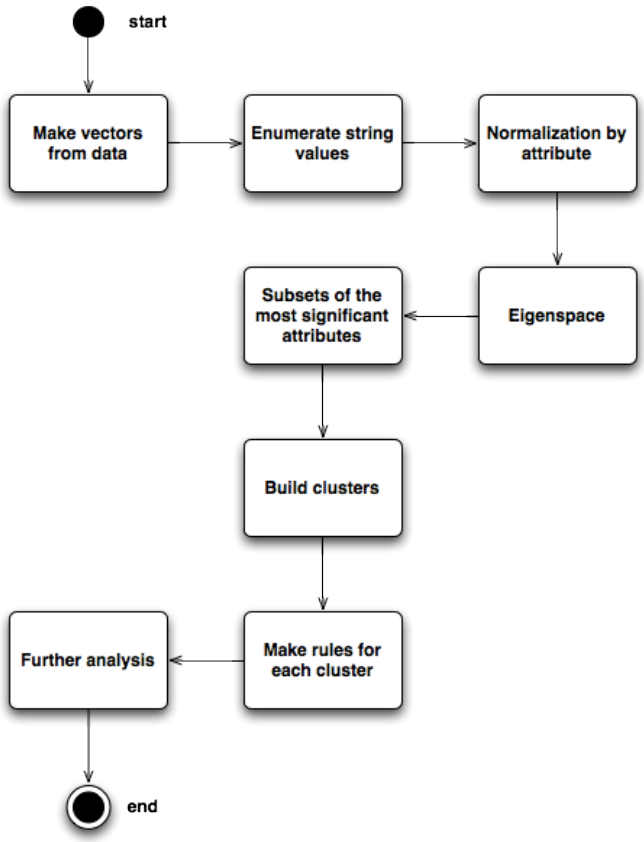
2.3.22.2 Classic Machine Learning

We experimented with several of the machine learning algorithms in order to get knowledge about the data. These algorithms were more thoroughly tested within WP3, using SAS software. Within the WP4 we tested the data and the results using a standard machine-learning package - WEKA. The datasets used were the NABIS live data and the rule driven synthetic data. Both datasets were directly fed into WEKA and only changed if the learning algorithm did not support types of the attributes.

2.3.22.3 Hybrid approach – Semantically driven Machine Learning

This section describes the algorithm that uses a constraint structure regarding the attributes of the dataset. The approach was tested using the a priori algorithm, implemented in WEKA, but modified accordingly. The attributes of interest are those that need to be present in the final description of some part of the space that rule describes. For our case, this means that at least one of these attributes needs to be present in the final rule that is presented to the expert. The rules of interest just show the basic form of cause-consequence. Again, this was the most practical approach for our test case algorithm, but can easily be generalized for other machine learning algorithms. The form of the rules of interest is: cause attribute list, consequence attribute list. This means that the cause and consequence attribute lists need to be present in the final rule that is presented to the expert.

The known rules are of the form: cause attribute-value list, consequence attribute-value list. These rules are therefore fully specified and already known to the expert. Their use can be to speed up the induction process or just to filter the results – there should be no such rules presented to the expert. Finally, we have unwanted rules – these are of the same form as the rules of interest, but always filtered out of the final rule set, presented to the expert. Semantics is being used to narrow the search and parameters which instances are being combined into larger vectors. The problem is that it is hard to determine which of the attributes are significant and how to group the data. Let us describe the approach we took to tackle the problem.



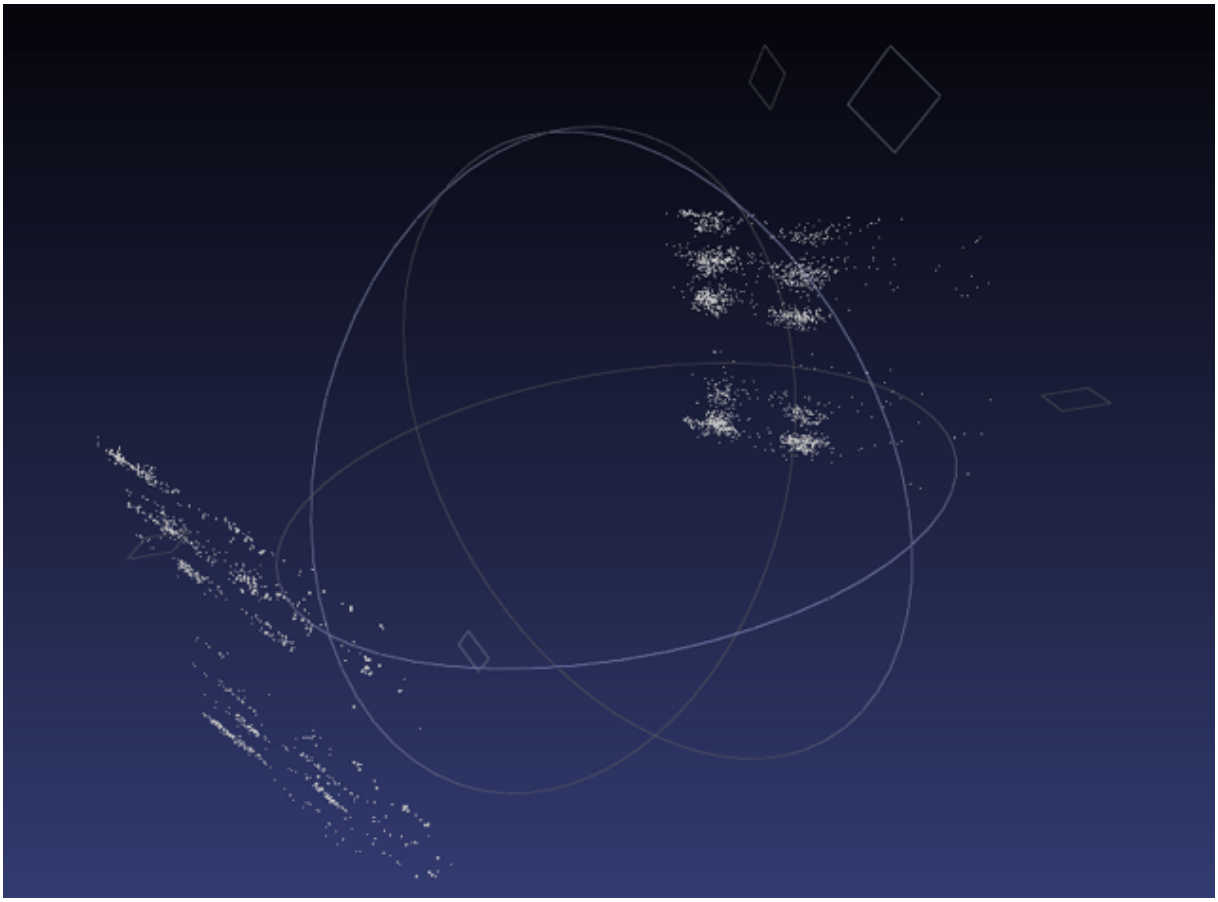
This is a short description of the process shown at the image above. In the first step, we create vectors from data. These vectors are either whole expansions, with all attributes, or selected subset. We then transform the values from words to integer, making the space discrete. The existing integer and decimal values stay the same. Then, the vectors are normalized by each attribute (not vector normalization), mapping all values of attributes in range of [0,1]. These vectors are then used to compute eigenvectors, eigenvalues and eigenspace. These values represent the attributes of the original vector that are correlated. We then use these subsets, to create new vectors, with only the values of attributes selected in the previous step. These subset vectors are then used to make clusters, using different clustering techniques. And then, for each cluster, the rules are constructed with classical machine-learning algorithms. These rules can be used to start further analysis of the data. It is important to state, that the most significant attributes can be used in combination with other attributes in order to explore new correlations and get new rules on the subsets. Looking at ballistic items (with incidents and locations), the following correlations are found:

- Correlation between incident location and ballistic item type,
- Correlation between incident type as well as location place,
- Correlation between start and end of investigation.

Some additional correlations found exploring the NABIS Gun data (expanded with ballistic item, incident and location):

- Incident type and gun type are correlated,
- Location of incident and location of found gun is correlated,

- Gun manufacturer is correlated with gun type.



The Odyssey Taxonomy is in the form of the OWL file, which can be easily edited and extended using open source Protégé tool. It currently consists of the most widely and preferred concepts available to the Consortium – the NABIS crime data structure and the FireTyDe ballistics information. It is, however, expected, that the technical standards, stemming from the research in the field of cartridge case and bullet comparison, we extended the current taxonomy. While the research in this area within the Consortium is appreciated, we do not expect to overcome the commercially available solutions. However, we expect to provide a building stone for open format and open comparison standards, using widely available tools, etc. and thus provide the Crime Laboratories across EU to efficiently share data and collaborate, while minimizing the costs of such collaboration.

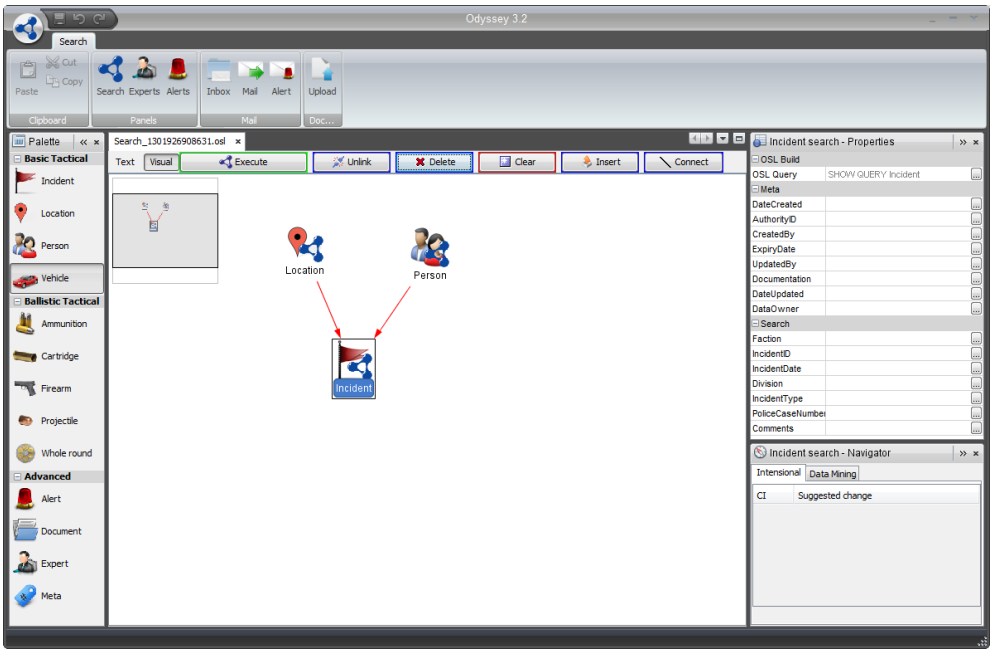
The data, available for testing of the pure semantic and semantically enhanced algorithms is rather limited. The real data, obtained from the NABIS system, was anonymized and has a large amount of missing values – using such corpora; the experiments with semantically enhanced algorithms would not yield any significant results. To this end, two sets of synthetic data were generated – the Odyssey data and the Rule driven generated data. The first one was generated purely for testing purposes of the Odyssey Platform, while the other was generated specifically for the tests with the semantically enhanced hybrid machine learning methods. One technically important result of the work is the implementation of the data flattening module, which would be used for transfer of the data within the Odyssey Database into the Odyssey modules, responsible for Machine Learning. Finally, we must note that large amounts of real data are needed for the final evaluation of the algorithms.

2.3.23 Visualisation

The Odyssey GUI (graphical user interface) was developed as a NetBeans IDE application. The platform enables to rapidly create desktop applications using the Java platform. It is free, open source, platform independent and stable. The NetBeans platform provided us with:

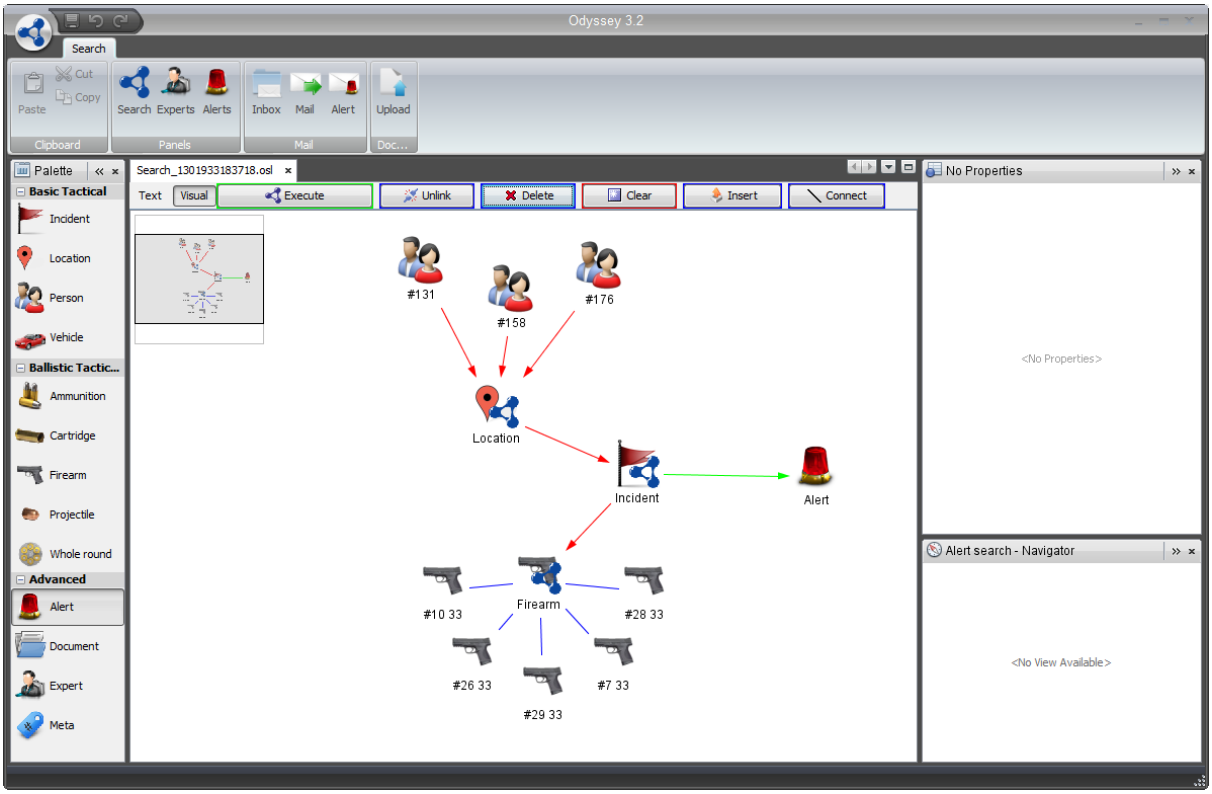
- **Modular architecture**: Only modules that have explicitly declared dependencies on each other are able to use code from each other's exposed packages. This strict organization is of particular relevance to large applications developed by engineers in distributed environments, during the development as well as the maintenance of their shared codebase.
- **Loose coupling & selection management**: The JDK 6 ServiceLoader class lets you load objects into a standard Java application's application context. The NetBeans equivalent, which is the Lookup class, provides the same functionality, dependency injection, and much else besides.
- **System File System**: Each module installed into a Swing application can install folders and files into the applications file system, allowing other modules in the application to find them and use them.
- **Window System**: Most serious applications need more than one window. Coding good interaction between multiple windows is not a trivial task. Out of the box, the NetBeans Platform provides functionality such as maximize/minimize, dock/undock, and drag-and-drop of windows in your application. That is made possible because windows in a NetBeans Platform application are part of the NetBeans window system.
- **Matisse GUI Builder**: Used to design Swing GUIs by dragging and positioning GUI components from a palette onto a canvas.
- **External open source modules**: Incorporated to extend the Odyssey platform with, for example, a PDF viewer or Microsoft Office 2007 ribbon menu look and feel.

The NetBeans platform is document centric, which means that a document editor window is a context for windows that support editing. The user interface consists of a few screens that constitute the Odyssey platform user interface.



The key feature of the Odyssey GUI is building graphical search queries and browsing results. Widgets used on the screens are reusable and their representation in a query language will be discussed later. The platform makes a full use of drag and drop features enabled in Java Swing and allow the user to build complex and reusable queries with a single mouse-click and link them holding a control button. An example search could look as follows:

The user drops a person to the search panel, sets ethnicity to white and gender to male. This allows the user to browse entries that are of interest and further narrow down the search. Furthermore the user interested in all incidents the selected people where involved in a certain area could drop a Location and an Incident widget, link the together and set constraints in the Location widget (see the properties window). The user can also further retrieve all firearms linked to the people, used within the location by connecting a Firearm widget to the Incident widget.



2.3.24 Domain-specific language

Domain-specific languages (DSL) express complexity at a particular abstraction tailored to both current and future needs. A DSL lets non-technical people understand the overall design of a platform and interact with it, using an understandable notation that reflects their particular perspective.

In the Odyssey project, a DSL was introduced to express the user requirements and solutions in a particular domain. A DSL promotes decoupling between components, modules and software stack layers, making the platform easily extendable and its components highly reusable. In the Odyssey project, a DSL language is used not only to convey the complexity of the domain, but also to facilitate and unify the entire communication across the platforms' components and users.

Odyssey's DSL compromises between the expressiveness of both a formal and flexible semantically-enhanced language. Complexity of syntax was greatly reduced by identification and categorisation of use case scenarios, grouping of functionalities and abstraction of data sources. Moreover, in contrast to, for example SQL, the user does not need to be aware of underlying data

structures, nor the platform's architecture, to enable a complex search to be undertaken. The user is asked to define the information of interest and the constraints by which the data will be filtered and sorted. In general, the user queries the system by defining the outcomes and under what conditions. One of the key requirements for the language is to facilitate access to factual information, but without taking the risk of misleading an investigator by presenting non-related data. The system reveals opportunities to the end user by facilitating discovery of new facts and collaboration on possible scenarios.

2.4 Validation

The objective of this phase of the project was the evaluation by end-users of the Odyssey platform in terms of use acceptability, performance, functionality, usability, and overall assessment. This phase started after the conclusion of the testing phase, when the platform has passed through unit, integration and system testing and was ready to be tested by end-users. This process gave the user time to run the Odyssey platform and verify it met the requirements that were specified in the first phase of the project. User validation helped us us also to filter out any bugs that need to be addressed concerning usability issues.

In order to guide users during the validation process, dedicated use case scenarios reflecting business objectives, which have been analyzed together with users' goals, were prepared. The Odyssey platform offers to users a system that supports their objectives, such as the ability to transfer and/or access technical or the ability to exploit automated and semi-automated processing and analysis of data or the ability to undertake data-mining and knowledge extraction, etc. Therefore users/stakeholders were interested in specific dimensions of evaluation in order to assess the achievement of their expected objectives in relation to the use of Odyssey platform to the process they are involved in. These user role preferences were taken into account when designing the user validation use cases, concreting specific scenarios depending on the user role objectives.

The real business users, who would have to operate the Odyssey platform in a real environment, performed this validation. As the key people who understand exactly what the business need is, and how it operates. Therefore they are the only people qualified to check Odyssey Platform to see if it does deliver any benefit to crime investigation.

Experts in different fields taken from both, the Law enforcement agencies already involved in the consortium such as such as Europol, UK Police Authorities, Royal Military Academy Department in Belgium, Republic of Ireland Police, Italian Police and external experts outside the consortium were invited to participate in this validation. Three validation sessions were held on users premises towards the end of the project where users with different profiles, from inside the consortium and external experts, were invited to validate Odyssey platform.

Though the overall acceptance and validation of the platform was high with users at an LEA tactical level and with both joint strategic and tactical users in the UK and Ireland. Some strategic users clearly see elements of the system as a challenge to their current role, as it puts analytical and data representational tools in the hands of LEA officers. Though the system was not designed for highly complex analytics. Some Europol strategic analysts see this as a shortcoming in contrast to their current tool set. It would be possible to add such components and it must be noted that it was not the intention of Odyssey to replace such tools (such as I2).

2.5 Standards

The project has identified a number of areas in which standardisation is both desirable and feasible.

2.5.1 Evidence recovery processes

The ways in which ballistics evidence in collected again varies in different jurisdictions. Standards could be implemented that recommend the best way to collect, label and submit ballistics evidence for analysis.

2.5.2 Data that should be recorded about a ballistics object

A ballistics object has many descriptive characteristics and some of these characteristics are used as a basis for searching in ballistics analysis technologies, crime recording systems and forensic audit tools. A specification of the minimum data fields that should be recorded about an object would lead to increased search efficacy and potentially better search results. Uniform names for data items could also be specified.

2.5.2.1 Data that should be recorded about a crime

Just as there are many characteristics associated with ballistics items, there are many characteristics of crimes. However, there are different ad hoc standards in place that determine the minimum data that is recorded about crimes and the format this data is stored in. Some systems will allow certain fields to be left blank and some systems will not. Similarly, some systems will also the user to enter free text whilst others will only allow a choice from pre specified options. This level of difference creates complexity when trying to extract intelligence from multiple disparate data sources. A standard defining the type and format of information recorded would be a useful first step in increased the efficiency of data mining.

2.5.3 Security standards for sharing data

Data sharing and security are intertwined for obvious reasons and there are general standards in place for the security of systems. The advantage of implementing ballistics data sharing on a wide scale is that the exchange of forensic ballistic data does not involve personal data. Therefore whilst the level of security needs to safely transmit and store this data is high, it is not as excessive as that for personal data. Sharing ballistics data is an ideal application to demonstrate the benefits of data sharing on a large scale and the required security architecture that should be in place. Much of this work has already been completed as part of the Odyssey Project.

2.5.4 Functionality of technology

Standards could be implemented that are effectively a specification for the functionality of any technology involved in the forensic ballistics process. It is known that all systems work slightly different and output data in different formats. However, standardising the functionality of technology would result in the end users directing the development of new features and ensuring the technical capabilities relevant to them are implemented.

2.5.5 Availability of technology

Crimes involving firearms are a problem 24 hours a day, seven days a week and 365 days of the year. It is important that when a crime does occur the relevant equipment is available. Standards could be implemented that specify the availability of the technology and the response times and response actions of the manufacturer in the event of a failure. Standards in this area could also cover secure backup and crisis recovery.

2.5.6 Compatibility / interoperability of technologies

A standard could be recommended that would form the first step towards full interoperability of technologies. Standards, legislation and requirements from end user work hand in hand in the standardisation process. The demand for a certain development or innovation can form the basis of a standard. If in this context there was a strong need for interoperability between different systems,

an agreement could be drafted that firstly outlines the desire for interoperability between systems and secondly describes a commitment to explore potential avenues to realise interoperability. This initial working agreement would be an official document upon which to base further work on interoperability.

2.5.7 Standardisation of legislation across Europe – what is a firearm?

The legal definition of a firearm varies between countries and standardisation efforts could be started to map the different legislative definitions in European Union countries. This could incorporate terminology and technical specifications of firearms and would help the streamlining of enforcement of laws and co-operation between different countries.

3 Potential impact

There are two areas of potential impact for the Odyssey project. The first is in the area gun crime detection and prevention. The second is in the broader area of cross European crime data exchange and analysis. The impacts from the specific technological elements have been explored fully in Section 2 above. This section will therefore focus on the potential impacts to gun crime detection and prevention.

The potential impact of the Odyssey project is best understood in the context of the impact that gun crime itself has on society. This section of the report has been prepared by and LEA partner – West Midlands Police. Gun Crime poses a significant and recognized threat to all Law Enforcement Agencies (LEAs) across the European Union and yet it only constitutes a very small percentage of actual crime committed. Provisional Government figures for 2009[6] in England and Wales showed that:

- 8,063 firearms offences were committed, accounting for just 0.2% of all crime across England and Wales.

Of these offences:

- Handguns were the most commonly used firearms, with the weapon accounting for over one-half of non-air weapon firearm offences recorded.
- Shotguns were used in 8% and rifles in 1% of these offences
- The statistics go on to show that the overall figure for gun-crime only rises to 0.3% of all crime if air-weapons are also taken into account.

Despite these relatively low numbers of offences, the public perception of gun crime is that it remains far more prevalent than these figures prove. This perception is often driven by the affect of media and local hype that surrounds such offences as will be demonstrated later in this section. The degree of misunderstanding of the true nature of gun crime by the public also leads this type of crime to being a major issue for politicians at all levels across society. Further, this can and does disproportionately affect the investment required to alleviate these fears. However, the potential cost, even in monetary terms alone, to society must not be underestimated. This too will be demonstrated here with figures from the UK Government that estimate the cost of just two high profile gun crime families residing in the Birmingham area of England.

3.1 Public Perception of Gun Crime

Many members of the public, and even some law enforcement officers and other associated staff, still see gun crime as predominantly a gang on gang or criminal on criminal issue. This perception often impairs the recording of events involving firearms and lowers the apparent desire to tackle the issues at source. Such perception can be extremely damaging to the objectives of governments and LEA's alike resulting in a reduced flow of key information and intelligence that can make the task of investigators and intelligence analysts far harder.

Whilst this perception is often true within communities and at the front-line of law enforcement, it is rarely true within strategic layers of policing and government. This is particularly so in the UK, where the effects of gun crime on communities and other innocent members of the public have been recognized alongside the economic costs to a society of failing to act proactively to reduce this type of violence. It's clear that gun crime has a disproportionately negative affect on the public's

[6] The Home Office Standard Note, SN/SG/1940, on Firearms Crime Statistics published June 2010

perception of crime and their neighbourhoods and communities. This sets gun crime out as a signal event that is ignored by all law enforcement and other relevant public bodies at their peril. Signal events are key indicators of the health, or otherwise, of a community and the investments in time and resources to deal with them effectively, whilst significant, are necessary to prevent escalation to far more serious issues and much greater cost in future.

3.1.1 Media Affect of Gun Crime

Gun crime attracts the press and generates publicity on a scale that is often rarely seen otherwise, as the case of Charlene Ellis and Letisha Shakespeare clearly demonstrates. These two young women were shot and killed leaving a New Year Party in Birmingham on 2 January 2003. Such events can and do trigger 'moral panics' in the media, becoming the focal point for extensive media coverage of a specific social or cultural issues – in this case gun crime.

A quick trawl of media and other websites reveals a plethora of material available to examine in the smallest detail almost every key incident that has occurred where firearms were believed, rightly or wrongly, to have been involved7. The Internet has also facilitated the wider dissemination of information from action, support and protest groups that have grown up around gun crime. These groups are able to take advantage of the capability afforded them by the web to lobby officials and create the necessary impetus behind their cause to demand recognition at higher levels of government than previously possible.

Social media also has a similar affect and this, in some ways, has again first been recognized by criminals. After a recent shooting in London, members of a criminal gang set up their own social media sites to warn off members of the local community who may have been considering contributing evidence, information and intelligence to the authorities to support investigation of the incident. It is essential that all LEAs recognize these forms of media and the potential they afford both criminals and LEAs alike across the globe.

The power of social media has never been more apparent than it has been in various Arab countries over recent times and it is extremely clear that it can equally be harnessed as a significant power for positive or criminal intent. LEAs must not miss such an opportunity or the initiative is likely to shift to or remain with those whose would use is for criminal purposes. The Internet and all it's capability is a threat to and an opportunity for LEA's and must not remain the domain of small numbers of isolated specialists or the true potential to use this technology to tackle gun crime will never be realized.

Using the Internet to facilitate effective communication between LEA's and the experts vested in the disparate disciplines of gun crime prevention and detection requires not only the harnessing of the technology but also a means for bringing together the differing cultures and vocabularies of all partners involved. Such exploitation of the Internet and modern technologies offers the chance for true interoperability, the harmonization of systems and processes, not only between LEA's across the EU but also across continents as the travel of gun crime is clearly not restricted to the EU alone.

3.2 Case Studies

The following case studies and description of the National Ballistics Intelligence Service in the UK are presented to demonstrate how these issues have impacted on local communities and the UK Government and the potential for improvement, and even cost saving, if the appropriate investment in resource and technology is made.

[7] See: Guardian online at: http://www.guardian.co.uk/uk/2005/mar/18/ukguns.ukcrime

3.2.1 Case Study 1 - The shooting of Charlene Ellis & Letisha Shakespeare

In the UK, the shooting of Charlene Ellis and Letisha Shakespeare, a single incident where innocent victims were caught in the crossfire of warring gangs, had more negative impact on public perceptions than a significant number of other such incidents that had happened over a good number of years previously.

Charlene Ellis and Letisha Shakespeare were shot and killed leaving a New Year Party in Birmingham on 2 January 2003. They were innocent bystanders caught up in the crossfire between the Johnson Crew and the Burger Boys, two notorious and violent criminal gangs based in the Birmingham area. The Johnson Crew and Burger Boys had been in violent dispute over their territories for many years that resulted, it is believed, in the death of a key member of the Burger Boys gang in December 2002. The victim's brother, believing the Johnson Crew to be behind the killing, planned his revenge. He recruited a number of people to assist in exacting that revenge, including the half-brother of Charlene Ellis.

Several items were obtained to assist with the revenge attack, including a red Ford Mondeo bought from Northampton. On the evening of the fatal party, the Burger Boys and their recruits drove up outside the salon where the party was taking place and "sprayed" the partygoers using a Mac10 sub-machine gun. This was an indiscriminate shooting because, although the intended target may have been present, the weapon, known colloquially as "spray and pray" because of its recoil, was almost impossible to aim with any accuracy. Clearly the criminals discharging such a weapon in public had little or no regard for anyone else caught up in the situation.

The national publicity that surrounded this incident and the ongoing trial over the following years resulted in a perception that was formed not only of gun crime generally, but of the local area involved as well as Birmingham as a whole. This negative perception was identified as a serious risk to local regeneration and potentially even the economic development of the whole region. It has been estimated by the UK Government that the two dynastic families, whose notorious gangs were responsible for these shootings, have cost the public purse over £37m8 in detecting and punishing their crimes over a period of 40 years. When the wider costs, including medical treatment etc., of dealing with the fallout of the gun related activity of these gangs are taken into account, this figure rises to a staggering £187m over 40 years.

This case also resulted in significant changes to the way trials were conducted and the processes that were permitted for the giving of evidence in British Courts. These changes permitted the giving of evidence by anonymous witnesses whose lives would otherwise have been put in significant danger and who might otherwise have felt unable to give the testimony that ultimately resulted in the successful prosecutions. However these changes did not occur easily within UK law and resulted in the loss of a high-profile murder trial at the Old Bailey in June 2008. The cost of that lost case alone was identified at £6m to the UK taxpayer and it was estimated that dozens of other cases were at risk of failing or being successfully appealed if UK law were not changed.

As a consequence of this, emergency legislation in the form of The Criminal Evidence (Witness Anonymity) Bill was rushed through both the Houses of Parliament and The House of Lords during July 20089. Without these changes to national legislation, it is likely that gun crime investigations and prosecutions would've continued to fail at early stages as witnesses felt unable to come forward.

---

[8] MailOnline at: http://www.dailymail.co.uk/news/article-1296682/37MILLION-Huge-taxpayer-crimes-just-TWO-families.html

[9] See MailOnline: http://www.dailymail.co.uk/news/article-1029045/Jack-Straw-plans-emergency-law-dozens-murder-trials-face-axe-anonymity-ruling.html

This is a prime example of how changing the law that surrounds both this and other types of crime can truly help in catching and convicting criminals. Such changes can also aid substantially in deterring criminals in future but they also highlight the need for the issues surrounding gun crime as a whole to rise for consideration and action by the highest authorities. Within the EU, the opportunity for travel across borders is a significant advantage to criminals wishing to commit gun crime directly or to facilitate it through others. In many cases, existing legislation, such as that relating to data protection, human rights and computer misuse, can be seen as a barrier to the sharing of information, evidence and intelligence that has the power to prevent and detect this crime, saving countless lives and serious injuries and substantially reducing the costs of such crime in the process.

3.2.1.1 Analysis

The above case demonstrates the impact that a single event can have on a community but also highlights the substantial cost of gun crime and it's associated criminality to the whole of society. It also demonstrates the need for the changing of laws where these are found to assist the criminals in protecting them from detection or prosecution. This event, along with a series of others that bore similarities were the reason for a review of gun crime being commissioned by the Association Of Chief Police Officers (ACPO). This review led, in turn to the establishment of the National Ballistics Intelligence Service within the UK.

3.2.1.2 Key Risks

What are the key risks not only for the public but also for the LEAs attempting to protect the public from gun crime? It is true to say that many members of the public tend to assume that LEAs already have the capability to share information, at will, across all borders and that they know everything there is to know about this sort of criminality. Obviously, this is not the case and, unfortunately, many too many criminals understand this only too well.

There are many examples of criminals using their knowledge of the frailties of LEAs and other government agencies to ensure they can continue to commit gun crime with much reduced likelihood of detection. This especially includes the now far simpler act of traversing borders within the EU. Obviously this reduces the deterrent effect of LEAs within Member States and increases the likelihood of further gun crime in future.

However, it's often not just geographic borders or contradictory legislation that separate information from those who would best make use of it. The differing disciplines of investigation, intelligence and forensic science can often create divisions within an LEA or even within an investigative team. Bringing these disciplines together in a way that ensured the whole was greater than the sum of the parts was a key objective of the National Ballistics Intelligence Service in the UK and has resulted in a step change in the way that gun crime is investigated and prevented.

3.2.1.3 NAtional Ballistics Intelligence Service (NABIS)

In 2007, a project to construct the National Ballistics Intelligence Service was commissioned within the UK on behalf of the England & Wales Association of Chief Police Officers (ACPO). The project was led from within the ACPO Criminal Use of Firearms Group after it was recognised that the existing framework for tackling gun crime had a number of built in barriers to improved performance.

The barriers to performance existed at both operational and strategic levels and required addressing across all criminal justice partners involved in tackling this type of crime. The key barriers identified were delays that were built into the process for obtaining evidence relating to potentially linked firearms incidents across the country, the inability of the police service to effectively share evidence and intelligence that had been gathered within previous investigations

and the reactive nature of gun crime investigations that resulted from the processes imposed as a consequence of these issues.

A decision was taken to build the new ballistics service, bringing together the disparate processes and providing a new database that could be updated and researched by all relevant partners. This involved working closely with all police forces and, in particular, those few that covered geographic areas that contributed most to the number of offences recorded across the country. However it was also necessary for the relationship between the police service and it's forensic providers to be re-examined in detail. This examination resulted in the conscious decision to bring some forensic examination services back under the direct control of the police service. Whilst this placed some strain on the relationship with the service, as it's forensic partners, this was managed proactively by engaging relevant members of each partner supplier to help them understand the need for change and the service that they would be asked to provide in future.

NABIS is delivered through four key centres, NABIS Hubs, based within strategic areas for gun crime, and a database delivered nationally alongside the UK Police National Computer. The NABIS Hubs are augmented by the NABIS Operations Centre and National Intelligence Cell based in Birmingham. This coverage provides a truly UK wide service. The NABIS Operations Centre coordinates activity between forces and disparate investigative teams as well as across countries where relevant issues are identified. They also provide administrative functions for the NABIS Database.

The NABIS Intelligence Cell provide backup to operational and investigative teams but also generate strategic reports from the database and other sources that analyse the effectiveness of NABIS activity as well as identifying up and coming gun crime issues that affect forces in the UK. These issues include the supply chain for weapons as well as other movement of firearms and organised gangs across geographic borders.

In the initial stages of constructing the NABIS service, the three key stakeholder groups of senior investigators, forensic scientists, including those from suppliers of forensic services, and intelligence analysts were brought together to gather their requirements against a newly identified core strategy. This new strategy is aimed at reducing the time taken for key information to be made available to investigators involved in recent incidents and the development of an approach to preventing future crime that focused on the knowledge that can be deduced and inferred from existing evidence and intelligence.

The disparity between purpose, language and culture of the three groups was highlighted during the requirements capture process but these sessions also offered the ideal opportunity to tackle those differences head on and find resolutions that would drive up the effectiveness of policing gun crime. The key objective of the scientists, for example and understandably, was to provide evidence to investigators of the links between recovered ammunition cartridges and/or weapons. The process required to produce evidential quality information from these items was detailed and relatively lengthy. Whilst the process could be accelerated in serious or high-profile cases, there was a considerable feeling among the investigators that earlier provision of this information could lead to improved opportunities for identification and conviction of offenders as well as reducing the likelihood of further offences by implementing interventions preventing retribution between gangs and other such retaliatory attacks.

Further review of these processes identified that the scientists were often able to give an opinion as to whether there were relevant links at an early stage of the evidential process, however they had previously been reluctant to voice these opinions for fear of doubt being cast on the scientific processes at a later stage or operational and investigative staff acting inappropriately on the information provided. The investigators and intelligence analysts, however, identified themselves as experts in evaluating uncertainty surrounding information and that the advantages of reduced

timescales for the development of intelligence, investigative strategy and tactics far outweighed the potential disadvantages that had been perceived by the scientists.

As the requirements came together, further opportunities were identified for the development of strategic information to guide and direct future crime prevention activity nationally and internationally. These opportunities included traditional management information as well as a change in focus from what was known (i.e. the recovered ammunition and weapons) to that which could be inferred (i.e. that there were other weapons, as yet unrecovered, that were available to criminals to continue committing gun crime). This switch of focus to identifying and tackling "inferred weapons" directly has greatly improved the effectiveness of gun crime investigation across the UK and has led to improved investigations, proactive operations and intelligence activity as far afield as the United States of America. The following two case studies demonstrate this change and the potential positive impact of such a cultural change on the way gun crimes are tackled by all LEA's.

3.2.2 Case Study 2 - The role of armourers in gun crime10

Figure 5: Recovered Firearms from Operation Newhaven

In late 2009 scientists from NABIS northern forensic hub in Manchester received cartridges from 3 separate crimes, in 3 different police force areas, with a distinctive ‘left rifling’ pattern that had not been seen before. This indicated that there might be a new ‘firearms factory’ or source of firearms supplying firearms for criminal use.

Based upon this information NABIS hosted a meeting between senior investigators from the 3 forces concerned and an intelligence sharing protocol was agreed. Operation NEWHAVEN was commenced to investigate the availability of firearms and ammunition in one of the force areas and concluded in early 2010 when officers recovered a sub machine gun and 3 self loading pistols from one of the main subjects of the investigation. As part of the operation a warehouse forming part of an engineering company was identified, 4 offenders were arrested and the premises were searched. A large quantity of firearms, associated paraphernalia and component parts were recovered during the search.

[10] Details provided by NABIS Operations Centre. Also see Liverpool Echo at: http://www.liverpoolecho.co.uk/liverpool-news/local-news/2011/04/20/liverpool-gun-gang-get-57-years-jail-after-uzi-and-glocks-seized-100252-28551038/

It became apparent that firearms were being reactivated within the premises using pre 1995 deactivated firearms as a base product for the process. In addition numerous 'Sten' guns were recovered in various stages of manufacture; it appeared that these guns were being manufactured from scratch within the premises.

An ammunition press and 200 rounds of ammunition were also recovered suggesting ammunition was also being produced at the premises. The ballistic material from the premises was submitted to the NABIS Northern Hub where the 2,000 rounds of ammunition were examined. As a result NABIS identified this gun 'factory' had produced at least forty-five reactivated or converted firearms. Potentially almost all of these items were sub machine guns. Four offenders have been convicted in relation to this operation and received a total sentence of 57 years imprisonment.

3.2.2.1 Analysis

This case study shows clearly the part that criminal armourers play in the supply and protection of firearms for serious and organised criminal gangs across the country. Without the supply chain being maintained, the availability of firearms and, in particular, the harder to obtain multiple discharge weapons, would be significantly reduced with the opportunity for death and serious injury ameliorated too. This case also demonstrates the ability of criminals to traverse the self-imposed boundaries of traditional policing, especially with the discovery of a link between one of the armourers involved and criminal activity taking place in the USA. The following case study shows this link clearly.

3.2.3 Case Study 3 - The use of travel as an aid to gun crime11

Following the recovery of the three self loading pistols from one of the main subjects of Operation Newhaven enquiries were made to try and trace the source of these weapons from the point of manufacture through the supply chain to the individual concerned. It was established that the 3 Glock pistols had been purchased by an individual in North Carolina, USA, using a credit card in his own name. In order to fully exploit the intelligence opportunities arising from this discovery, ownership of the investigation was passed to a Regional Task Force covering a number of police force areas. This presented an opportunity for enhanced levels of intelligence sharing across police forces during the operation. One of the first things that the Task Force did was to establish operational interaction with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) in the USA.

Enquires made by the ATF established that the suspect had travelled to the UK on numerous occasions in 2010. It is apparent that during these trips to the UK the suspect was carrying firearms in his stowed baggage. The suspect was placed under daily surveillance in the USA, during which he was seen to purchase 16 x 9mm Glock pistols. In the summer of 2010 he was tracked to a North Carolina airport where he checked in four bags, he did not declare any firearms inside his luggage. The luggage was intercepted and found to contain sixteen firearms and thirty-two magazines. The suspect was arrested and detained in custody in the US.

During the surveillance the suspect was seen to dump thirty-three Glock Security Boxes supplied with the firearms, ATF Agents collected these. Along with the boxes and other associated items were a number of fired cartridge cases. Eighteen of these cartridge cases were flown to the UK where they were added to NABIS' Integrated Ballistics Identification System (IBIS). In autumn 2010 one of these casings was matched by NABIS to a shooting incident in Greater Manchester where an individual was subject to a non-fatal drive by shooting. In a subsequent search relating to this incident, four further firearms where found at an address in the force area. One of these firearms was a Glock 26 pistol that was purchased in the USA and is subject to another on-going

[11] Details provided by NABIS Operations Centre

investigation. The other three firearms were unrelated; however NABIS analysis shows that two of the firearms are connected to eight firearms discharges in the North West going back to 2000.

3.2.3.1 Analysis

Examination of this case study shows not only the ease with which some criminals are able to obtain firearms and ammunition in foreign countries before returning to their own or another country to supply them, but also the readiness of such people to do so in full view of the authorities. As is often the case, it was the intelligence surrounding this individual that offered a context that facilitated his arrest and prevented a myriad of weaponry from being available to commit gun crime.

3.3 EU Opportunities

The success of NABIS in the UK has prompted consultation within the EU into ways in which the lessons learned in the UK could be could be combined with experiences with the region and propagated to all Member States, thus raising the bar for the tackling of gun crime across the whole of the EU. It became very clear during this wider consultation, with experts from each of the disparate law enforcement disciplines, that the sharing of ballistic, crime and intelligence information and the ability to analyse it effectively remained a key blocker to improving the fight against gun crime across EU borders.

The legal frameworks that exist within individual Member States and the variation in approach and culture between them further complicate this situation. The disparate technologies that are used by LEAs and other scientific establishments to record crime, intelligence and ballistic classification and imagery information add to this confusion rather than reduce it. The requirements that were articulated as a result of this consultation thus had a substantial emphasis on the need for open standards that are essential to breaking down barriers such as those identified in order to assist the effective fight against gun crime. It would be foolish to attempt to address any of the cross-border issues without taking into consideration the need for levels of security that are commensurate with the crimes being tackled.

3.3.1 Information Security

Obviously, where threat to life and, in some cases, many lives is involved, the information and intelligence that surrounds these people and events must be protected sufficiently to substantially reduce the likelihood of compromise that may raise the risk of further harm rather than lower it. All of this must be done in a way that is seen to protect the public whilst building in “privacy by design” and "proportionality" within system and process. Within the UK the NABIS Database has been accredited as CONFIDENTIAL under the Government Protective Marking Scheme (GPMS). This designation has a significant impact upon the storage, use and dissemination of information that impacts squarely on cost and timeliness if not managed effectively. Without all of these factors being fully appreciated and adopted within any proposed EU wide solution, confidence would remain low and leave that solution lying unused on the proverbial shelf, where it can little afford to be.

3.3.2 Cost

Whilst considering other potential blockers to systems and processes, it is important to address the potential cost of a system designed and built to address all of these issues, especially at a time of austerity for all Member States of the EU. It’s a fact that all LEAs are seeing budgets cut and staff reduced. Efforts are being made to maintain front-line services but the definition of these can often be difficult. Whilst it is not expected that anyone would not see gun crime as a front-line issue, there may be doubt about some of the services that are believed by LEA's to be essential to supporting it. It's also essential, therefore, that any development to tackle these issues takes into account the affordability of any potential solution for all LEAs across the EU and that every opportunity to

automate processes and outcomes be taken to minimise the impact of reducing resources imposed on those LEA's.

3.3.3 Future of Managing Gun Crime Information

Technology and informatics has advanced greatly over recent years and is likely to continue to do so for the foreseeable future. The understanding among practitioners, scientists and academics of the chaotic nature of gun crime has improved substantially and will go on doing so with improved methods of information capture and analysis. The sciences of Emergence and Complexity offer the opportunity to determine key links and signals from a wealth of data and information available to modern investigators and strategists alike. Automating these processes will enable front-line resources to be tasked efficiently to tackle this most serious of crime types.

3.3.4 Future Solutions

It is into the landscape described in the above paragraphs that any new system and/or technology, such as that proposed by the Odyssey Project would be introduced. This is a complex and fast moving landscape that will demand the best of academics, technologists, strategists, business experts and politicians alike if systems and processes are to be made truly interoperable and capable of functioning effectively across the EU to tackle gun crime.

3.4 Conclusion: users and standards

The Odyssey prototype has demonstrated the potential advantages for end users of a pan-European ballistic crime system. To transform this into a fully operation system deployed within a key EU body (for example EUROPOL) with support from the full range of EU LEAs would require a number of key next steps – most of which are not technology challenges. These can be grouped under: users; standards and policy.

3.4.1 Users

The user studies within the Odyssey project have identified three key *roles* but multiple *jobs* with different goals within the various member state LEAs with regard to ballistic crime detection and prevention. The three roles broadly defined are:

- Investigation
- Ballistics and forensics
- Analysis

Each role has differing goals and hence relationships to crime data. Investigators are primarily concerned with the operational and tactical use of data. They are looking for hints, tips, leads and intelligence which may lead to best routes of enquiry. They are not looking for evidential quality links in data, nor are they often looking to broad overviews of ballistic crime. Forensic officers are more concerned with evidential quality data and establishing firm links between items, especially when looking to support prosecution of offenders. Analysts are looking to the broad strategy overviews of data which support policy and policy based actions. These are of course broad-brush representations of the observed user practice and roles which may not map on to specific jobs within specific LEAs. In a small number of notable cases, especially in the LEAs of smaller member states, all three roles may be undertaken within the job of one or a set of post holder, who may also be serving police officers. In other cases each role has become specialised within the organsiation. The Odyssey system has sought to provide solutions to these various potential end users. A full implementation would require further work to ensure the system provided full functionality to for each role and flexibility to integrate into different LEAs organizational structures.

3.4.2 Standards

With regard to standards considerable work remains to be done in defining these and implementing them through policy actions within the domain of ballistic crime data within the EU:

- There are no accepted Open standards for data capture, processing and representation in original and meta-data forms
- There are no accepted Open standards for comparison, audit, and regulation of system usability, performance and reliability

These points hold for both ballistic imaging and matching systems and for ballistic crime BIS. There remains the potential for a de facto standard to come into force via the market dominance of one product or range of products, or through a merging of common practice within larger member states or LEAs. At the time of writing the opposite processes appear to be taking place. The market for ballistic imaging and matching systems is growing and there is evidence of fragmentation in operational practices within larger member states The XML schemas used within the Odyssey platform could provide an initial template for such a standard within the domain of ballistic crime. Having said this data standards for ballistic imaging systems and standards for processes of data acquisition have yet to be established. The current market for such systems does not support the development of open standards and may require policy intervention. Further outputs from the joint work between the Odyssey project and ENFSI may provide some grounding for such standards.

3.4.3 Policy

As noted above there is a very strong policy framework in the EU for high quality data exchange between member state LEAs – as defined by the Swedish Initiative, the principal of availability and the Prüm decision. The implementation of this policy will require extensive and further investment in relevant research and development projects (of which Odyssey represents one such project) as well as infrastructure developments within, between and among member state LEAs. From the user and contextual research undertaken by the Odyssey project a key policy development has to be that of identifying, defining and establishing key standards for data exchange.

3.4.4 Next steps

As an information system the Odyssey platform demonstrates the possibilities for EU member states in combatting gun crime through a pan-European approach to sharing data. The system incorporates the use of advanced data mining techniques enriched with semantic technologies. It extracts information from various data sources and indicates how the information will be used next. Moreover, it creates an ontology-driven knowledge repository that enables the analysis of information in a more abstract way, which gives an advantage of being able to illustrate global tendencies or crime patterns. Odyssey platform uses a novel approach for incorporating dynamic user requirements into system realisation (i.e. OSL). The repository is used to operate and investigate real cases using logic reasoning and knowledge interference. Additionally, the platform is able to generate unified graphical results and clearly demonstrate the outcomes of complex analysis. Finally, the platform operates on a very specific domain, which enables the concentration of explicit problems, constantly evaluating outcomes, and suggesting the most promising solution.

The fully implemented version of the platform has the potential to fill a major gap in cross-national investigation and security systems. National police forces would be able to increase their investigation potential by accessing the refined data and graphically represented data patterns. Moreover, the Odyssey platform is structured as a framework which could be easily replicated for other forensic data sets as well as applied to different domains, thus re-defining the standards of information exploitation for large data sets. The latter provides a major millstone for truly integrated and pan-European law enforcement knowledge management Systems.

3.5 References

Interpol, 2007. Connecting Police: I-24/7. Available at: http://www.interpol.int/Public/ICPO/FactSheets/GI03.pdf. [Accessed February 3rd, 2011]

Europa, 2002. Proposal for a Framework Decision on exchange of information under the principle of availability. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/367&format=HTML&aged=0&language=EN&guiLanguage=en [Accessed January 25, 2011].

Prüm, 2010. Prüm Decision. Available at: http://ec.europa.eu/home-affairs/policies/police/police_prum_en.htm [Accessed January 25, 2011].

NABIS, 2009. National Ballistics Intelligence Service. Available at: http://nabis.police.uk/database.asp [Accessed January 25, 2011].

Akhgar, B et al., 2009. A Pan European Platform for Combating Organized Crime and Terrorism (Odyssey Platform). In Centeris Conference on Enterprise Information Systems. Ofir, Portugal.

Akrivas, G, Wallace, M, Andreou, G, Stamou, G, Kollias, S, Context-Sensitive Semantic Query Expansion, in Proceedings of IEEE International Conference on Artificial Intelligence Systems (ICAIS'02. pp 109. 2002 .

Bonino, D, Corno, F and Farinetti, L, 2004. Domain specific searches using conceptual spectra. In 16th IEEE International Conference on Tools with Artificial Intelligence. ICTAI 2004, pp. 680-687.

Bundeskriminalant, 2004. Firearm Type Determination. Available at: https://www.forensic-firearms.bund.de [Accessed January 25, 2011].

Chen, H. et al., 2004. Crime data mining: A general framework and some examples. IEEE Computer, 37(4), pp.50-56.

Chen, H. et al., 2003. COPLINK: managing law enforcement data and knowledge. Communications of the ACM, 46, pp.28–34. Available at: http://doi.acm.org/10.1145/602421.602441.

De Bruin, J. S. et al., 2006. Data mining approaches to criminal career analysis. In Proceedings of the Sixth International Conference on Data Mining. Sixth International Conference on Data Mining. pp. 171-177.

Fowler, M and Parsons, R., 2010. Domain-specific Languages, Addison Wesley.

Giacomo, G, 1996. Intensional query answering by partial evaluation. Journal of Intelligent Information Systems, 7:4, pp 205-233. Published by Springer Netherlands, Nov. 1996.

Jopek, L., Wilson, R., and Bates, C, 2010. An application of a domain specific language facilitating abstraction and secure access to a crime. In Proceedings of IARIA 2010. pp 29-33, Lisbon, Portugal, October 2010.

Mernik, M., Heering, J. & Sloane, A.M., 2005. When and how to develop domain-specific languages. ACM Comput. Surv., 37, pp.316–344. Available at: http://doi.acm.org/10.1145/1118890.1118892.

Nath, S. V., 2006. Crime pattern detection using data mining. In Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. International Conference on Web Intelligence and Intelligent Agent Technology. pp. 41-44

Nygren, F, 2008. The Swedish Initiative. http://www.daten.european-police.eu/2008/nygren.pdf [Accessed January 25, 2011].

Sims, C, 2010. National Ballistics Intelligence Service Update Report. Available at: http://www.west-midlands-pa.gov.uk/documents/committees/public/2010/12_PerfandOps_22April2010_National_Ballistics_Report.pdf.

Smith, M. and Tilley, N. 2005. Crime Science: New Approaches to Preventing and Detecting Crime, Portland, USA: Willan Publishing.

Strohmaier, M., Kröll, M. & Körner, C., 2009. Intentional query suggestion: making user goals more explicit during search. In Proceedings of the 2009 workshop on Web Search Click Data. WSCD '09. New York, NY, USA: ACM, pp. 68–74. Available at: http://doi.acm.org/10.1145/1507509.1507520.

Vallet, D, Castells, P, Fernández, M, Mylonas, P, and Avrithis, Y, 2007. Personalized Content Retrieval in Context Using Ontological Knowledge. IEEE Transactions On Circuits And Systems For Video Technology, 17:3. MARCH 2007.

Wilson, R., Jopek, L., and Bates, C, 2010. Sharing Ballistics Data across the European Union. In Proceedings of IARIA 2010. pp 8-13, Lisbon, Portugal, October 2010.

Yates, S., et al., 2009. Semantic Interoperability between Ballistic Systems through the Application of Ontology. In IADIS WWW/ Internet Conference. pp. 153-157.

Yu, L., 2008. Prototyping, Domain Specific Language, and Testing. Engineering Letters.

4 Publicity information

4.1 Odyssey Contact Details

Odyssey Co-ordinator

Prof. Simeon J. Yates
Professor of Communication and Technology
Director Cultural, Communication and Computing Research Institute
Director Design Futures Centre of Industrial Collaboration
Tel: +44(0) 1142256775

Fax:+44(0)1142256702
E-mail: s.yates@shu.ac.uk

4.2 Odyssey Beneficiaries

Beneficiary Name	**Country**	**Contact Name(s)**
Sheffield Hallam University	United Kingdom	Professor Simeon Yates
Atos Origin	Spain	Pedro Soria Rodriguez
Forensic Pathways Ltd	United Kingdom	Richard Leary
EUROPOL	Netherlands	Sven Lemmens
XLAB	Slovenia	Gregor Pipan
MIP Consorzio Per L'innovazione Nella Gestione Delle Imprese E Della Pubblica Amministrazione	Italy	Claudio Palasciano
West Midlands Police	United Kingdom	Gary Herrington
Royal Military Academy	Belgium	Alexandre Papy
An Garda Siochana	United Kingdom	Kevin Brooks
SAS Institute	United Kingdom	Geoffrey Taylor
DAC Servizio Polizia Scientifica	Italy	Federico Boffi
North Yorkshire Police	United Kingdom	Dave Fortune

4.3 Odyssey website

http://odyssey-project.eu/

4.4 Odyssey logo

A new logo was developed during the first months of the project and this is the Official Odyssey Logo. It is used on both internal and external documents.

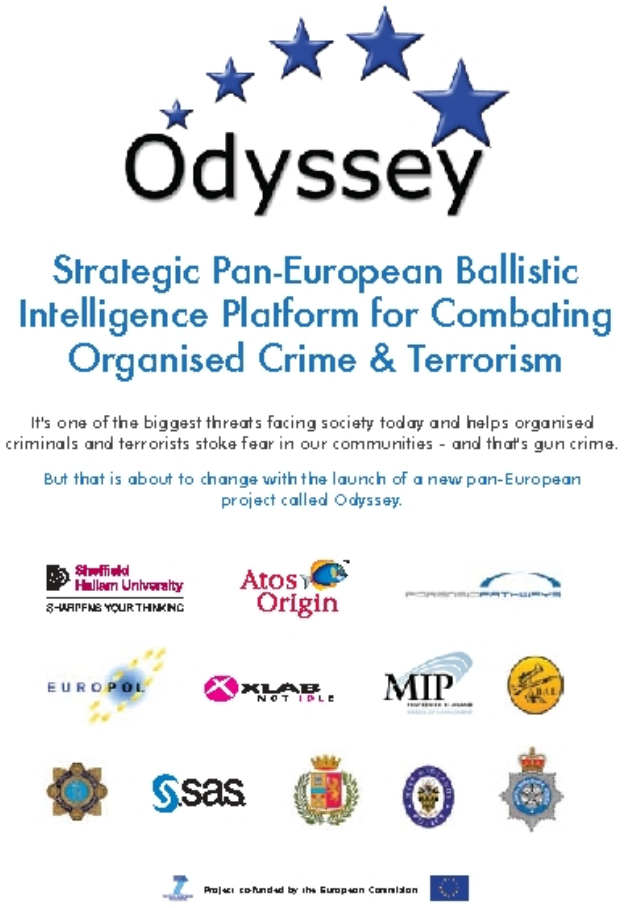
4.5 Odyssey Publicity

All of the below publicity aids have been distributed and shown at a range of conferences across Europe.

4.6 Odyssey Newsletters

Click on the each image to view full newsletter

4.7 Odyssey Leaflet



Co-ordinated by Sheffield Hallam University in the UK, the project is a collaboration of police experts, industrialists, computer scientists and researchers working together to develop a secure interoperable situation awareness platform. This will enable the automated management, processing, sharing, analysis and use of ballistics data and crime information to combat organised crime and terrorism.

The Odyssey project, launched in the autumn of 2008 is part funded by the 7th European Framework Programme for Research and Technological Development. The project will use non-personal ballistics data and crime information to identify connections and links that previously would not have been discovered. This will allow police forces to co-operate on cases and pinpoint similar crimes which could be related.

Experts will examine the bullet casing and/or the related firearm to assess the 'toolmarks' on the evidence. Each gun leaves a different 'signature' on a bullet fired from it.

Using this data, it is hoped that police forces will be able to track guns from crime-to-crime, and possibly from country-to-country, and by doing so will find out which criminal or terrorist networks have been using the weapon.

The Project will conduct research and create a secure pan-European ballistics and crime information intelligence network not only to tackle organised crime and terrorism but also to increase the safety and security of all EU citizens.

Professor Simeon Yates, Director at Sheffield Hallam University's Cultural, Communication and Computing Research Institute (C3RI), is co-ordinating the Odyssey project.

He says: "Security agencies have been using ballistics data for many years but, until now, they have been acting in isolation. This system will automatically alert relevant agents in other countries when there is a match on gun and bullet signatures".

"Criminals use guns as currency, and Odyssey allows agencies to build profiles of crime networks by tracking the unique 'signature' that guns and bullets produce when they are fired."

One of the driving forces behind Odyssey has been EUROPOL, the European law enforcement organisation. Other partners involved in the development include the National Ballistics Intelligence Service (West Midlands Police is the lead police force), North Yorkshire Police, the Royal Military Academy, SAS Software Limited, the Politecnico di Milano, Garda Siochana (Irish police), the Italian police force, XLAB, Forensic Pathways Ltd and Atos Origin.

Email: aces-odyssey@shu.ac.uk
http://odyssey-project.eu

Sheffield Hallam University
Tel: 44(0)114 225 6787

4.8 Odyssey Exhibition Stand

Odyssev Poster