



**EUROPEAN COMMISSION
DIRECTORATE-GENERAL OF JUSTICE AND
HOME AFFAIRS**



**A EUROPEAN NETWORKED FIREARMS
INTELLIGENCE DATABASE**

CONTACT
Dr Richard Leary
Forensic Pathways Ltd
19B Sandy Way, Amington Industrial Estate, Staffordshire B77 4DS, United Kingdom
Phone/Fax
Phone +44+(0)1827+312812
Fax +44 (0)1827 312912
Cell +44 (0)7919 548405
Rleary@forensic-pathways.com
www.Forensic-Pathways.com

ACKNOWLEDGEMENTS



This work was commissioned by The Homicide Working Group at EUROPOL and funded by under the AGIS Programme; a framework to help police, the judiciary and professionals from the EU Member States and candidate countries co-operate in criminal matters and in the fight against crime. We are grateful in particular to the Deputy Director of SOCA Mr Andre Baker who initiated this work, Commander David Johnston Head of Homicide and Serious Crime Command, Specialist Crime Directorate, New Scotland Yard (Chairman of EU Homicide Working Group), Deputy Director of EUROPOL Mr Kevin O’Connell and Detective Inspector Ian Pegington of New Scotland Yard (Homicide Working Group). Their support, guidance and advice in the preparation of this Report was invaluable. Without their assistance this Report would not have come to fruition.

**Dr Richard M Leary, MBE, LLB Hons
Forensic Pathways
March 2007**

BACKGROUND

Forensic Pathways was Commissioned by the Homicide Working Group at EUROPOL to assess the feasibility of developing a Pan European approach to the management and use of forensic ballistic evidence and intelligence across the European Union (hereafter EU).

The purpose of the study was to assess the potential impact of the management of ballistics evidence and intelligence on controlling and reducing organised crime across the EU in accordance with the EUROPOL Convention. The Convention states:

“To improve police cooperation between Member States to combat terrorism, illicit traffic in drugs and other serious forms of international crime.” In undertaking this research and writing this Report attention has been paid to the Conventions Principle Tasks for EUROPOL namely:

- The exchange of information between Member States;
- Obtaining, collating and analysing information and intelligence;
- Notifying Member States without delay of information concerning them and of any connections identified between criminal offences;
- Aiding investigations in Member States;
- Maintenance and use of computerised systems to collect information.

This Report focuses on two specific areas of work by EUROPOL;

Firstly, the EUROPOL Homicide Working Group in focussing on the prevention of organised crime, including homicide and especially in relation to people from vulnerable groups where firearms are involved; Secondly, the work of EUROPOL in focussing on better ways to manage and use ballistics evidence and intelligence across the EU in support of its Principal Tasks.

The work was divided into three broad pieces of activity:-

1. Firstly, an **Interim Report** which set out the basic foundations of the study, along with a range of initiatives that could be adopted to significantly improve and enhance what currently exists.
2. Secondly, a **Research Period** in which key individuals and organisations were consulted across the EU to establish their needs and gain views about opportunities and barriers. Research was also conducted into better ways of managing evidence, intelligence, systems and techniques to improve performance.
3. Thirdly, a **Final Report** to bring together the work as a whole and Report recommendations from the research.

The Interim Report

The Interim Report was accepted by the Homicide Working Group in 2005. It was subsequently recommended by the Deputy Director of EUROPOL Mr Kevin O'Connell to the European Commission as a valuable foundation for the development of an Information Strategy for EUROPOL and a shared European Firearms Database.

Research Period

The research period in 2005 and 2006 included visits and communications with Member States law enforcement departments to gain insights into their views about the adoption of the foundations set out in the Interim Report.

Final Report

The Final Report is the product of the work as a whole and outlines key features of the project. As a result of the acceptance of the Interim Report and the acceptance by EUROPOL of the Findings, it is recommended that a shared European Networked Firearms Database be established.

MEMBER STATES CONSULTED

The following Member States each received a copy of the Interim Report and were consulted about the contents:

- Portugal
- Spain
- France
- Italy
- Greece
- Slovenia
- Czech Republic
- Poland
- Holland
- Belgium
- Germany
- Sweden
- Denmark
- Finland
- Estonia
- Ireland

Senior investigators from the police service visited and consulted with staff in Member States to obtain their views about the Interim Report and Questionnaires were circulated. These were fed back into the research project. Dr. Leary visited the BKA in Germany and West Midlands Police in the United Kingdom where a new interoperable national system is in the process of being developed. A copy of the Questionnaire circulated can be found in Appendix 1 at the rear of the Report. The overwhelming view of respondents was in support of the proposal that there should be a European Union Networked Firearms Intelligence Database. This was reiterated in

EUROPOL at the Homicide Working Group consultation process in March 2007.¹

BALLISTICS AND CRIME LINKING

Firearms have markings left on the internal working parts of the weapon during manufacture. They also have markings on the outside of the weapon to denote brand and identity. When bullets are fired from a weapon 'striation' marks are left on the outer surface. The cartridge case also has unique markings left upon it via the striking of the firing pin and the use of ejector pins to extract the case from the weapon. These marks provide two important characteristics used in forensic ballistics each of which is the opposite of the other; firstly they are *highly discriminating* between bullets and cartridge cases so forensic experts can conclusively state that two objects are not associated and secondly, they can provide *convincing evidence of association* so forensic experts can say that the two objects were discharged from the same firearm.

This enables the firearms examiner to:-

1. Directly match or distinguish between two or more bullets as having been fired from the same weapon
2. Directly match or distinguish between two or more cartridge cases
3. Directly match or distinguish between Test Fired Bullets and Cartridge Cases with recovered samples

In addition to this simple form of linking crime cases described there is a more sophisticated method that can be used to link series of crimes in more subtle and sometimes complex ways. See Appendix 2 for details and

¹ Mr Kevin O'Connell. Deputy Director EUROPOL.

illustrations. This technique involves the use of combinations of 1 – 3 above to link crimes in a network of both direct and indirect correlations.

Figure 1 – 9 in Appendix 2 illustrates how crimes can be linked and complex associations between events identified. The illustration is a Matrix of Crime Scenes and Firearms used to develop extended links that would not normally be identified. The Matrix illustrated illustrates the approach advocated in this Report namely a Networked Firearms Intelligence Database.

In the example shown in Appendix 2 only a small number of Crime Scenes have been used to demonstrate a simple example. However, this approach can be used with vast numbers of Crime Scenes, pieces of evidence and firearms. The Matrix illustrated has only 10 Crime Scenes, 12 Firearms and a range of ammunitions. The process described can be computerised and used within a secure and trusted interoperable network. Security was one of the main causes for concern for respondents and is dealt with later in this Report.

The work to develop and test this technique has also been tested with a substantial dataset. The dataset involved was a batch of 32,000 pieces of evidence from South Africa.² Links similar to those described in Appendix 2 were identified. Notably one unsolved Murder was uncovered and the evidence and passed to the investigating officer. This demonstrates the implicit power of the approach. The technique described in Appendix 2 is the technique envisaged for use in the EU and although there are many technical hurdles to overcome these can be dealt with as part of a later project.

Consultation Process

Respondents recognised unanimously the importance of European Co-operation. All said they would recommend this to their respective

² We are grateful to the Government of South Africa and the police service for their active assistance in access to this non-personal technical data.

The Table in this example illustrates a sliding scale based on a measured factor of efficiency and the number of items of evidence in the database. It will be seen that 5% efficiency at 'Match Yield' in a database of 1 Million items results in 50,000 investigation leads or 'Matches'. This raises many issues about 'efficiency and process management' that need to be capitalised upon. It also raises issues about the way in which efficiency is currently measured. At present efficiency is calculated simply as a count of how many 'Matches' are gained by a Laboratory or Unit and this can be misleading. Many variables affect efficiency including how many items of evidence are recovered and entered into the database, how many guns are examined and demographic variables. There are of course many other performance measures that could be introduced to assist in raising efficiency, solve crime and increase security.

Some respondents stated that only those recovered firearms suspected of involvement in crime are examined whereas others said most recovered weapons are examined. It is recommended that this be made a policy matter for consideration by the Working Group. When asked about how officers decide which weapons are to be examined the common answer was that it is based on experience. One said that decisions are based upon the officers' belief in how busy the firearms examiners are. One offered to supply the Member State policy.

One member said that they examine 5,000 – 6,000 cases currently and get 60 – 80 matches annually. However in the 1990's they examined 10,000 – 15,000 but had a backlog of 35,000 cases. The numbers of successes were unavailable. Other estimates varied and it was soon appreciated that performance measures are not standardised. Some Member States have been given Awards by a supplier for reaching certain targets in matches but these are not assessed against any control measures. For example the number of examinations conducted, the number of crimes involved, number staff employed and the time scales involved. Without these the statistics

results can be misleading and sometimes lead to inefficiencies and bad practice. It is Recommended that consideration be given to more meaningful Performance Indicators.

Members were asked about the linking of series of cases using ballistics evidence. There was an overwhelming response indicating that cases are examined on the basis of single links. This means that crime is not always considered in series or networks of links. It is Recommended that this perception and the limiting beliefs it involves should be addressed by the Working Group. Crime is a social phenomenon and as such exists in networks of associations in and between criminal groups. Networks are relatively easy to identify if rigorous systematic approaches are taken to collecting the data and analysing it.

One issue of interest that was raised by a number of members was how it was proposed to examine pieces of evidence without the original exhibit i.e. the bullet or cartridge case. One respondent said special arrangements would be needed for the release of an 'original' and this he thought could present problems. He was happy to share data however. When asked if he would be happy to consider correlation requests and examine copies he agreed that as an examiner he would. Comments are made later about perceptions of continuity requirements and legal compliance issues.

One respondent raised the same problem and posed a situation where there are three cases suspected of being linked. For example cases in Paris, London and Dublin. In that situation who would be given which pieces of evidence? It is recommended that this is a policy matter for consideration by the Homicide Working Group.

Some examiners made comment about whether the examiner or scientist should be a generator of intelligence. By this it was meant whether they should look at the dataset as a whole to develop links to any crimes in the

system. Different people said slightly different things about this but there is a perception issue about roles and responsibilities that requires clarification and harmonisation. Moving into a more intelligence led environment requires different thought processes and considerations and some of these could be culturally based. It is recommended that consideration be given to addressing this.

Different perceptions exist in some Member States about what 'evidence' actually is and what 'intelligence' actually is. The line between them is sometimes blurred depending upon which Member State you speak to and even which member of staff. The legal tradition and philosophy of law in some Member States affects this perception and should be considered further. Building a network across the EU would bring this into focus and it requires consideration. One respondent said that the original piece of evidence must always be available and he is only concerned with the case "in front of me at any one time". It is Recommended that the Working Group consider the forensic harmonisation issues in the EU that this presents.

One respondent specifically stated that he would have reservations about a central database of all information at EUROPOL but would support a distributed network of the data. The same respondent said that he was concerned about the state of the data and would seek assurances it was 'clean' if it were to be shared.

One respondent said that the problems surrounding the use of technical equipment for example IBIS should be separated from the problems of managing an EU network and developing an analytical capability. This examiner said that IBIS the main system employed was not built for intelligence purposes rather it was for the comparison of images. Systems like IBIS assist the firearms examiner sort and sift evidence for comparison and in the process of so doing collects and stores data. It can therefore have a role in the supply of data for intelligence purposes – a function these

machines are currently not designed to undertake. Although the machine serves the purpose of collection and storage of images the data collection can be used for advanced analytical processing as well. Important here is the development of a data sharing capability, an analytical function and a trust and security management platform.

When asked what barriers there were to sharing by far the most common responses were:

- 1) Legal – Different legal approaches
- 2) Physical Barriers – Need the original exhibit or communicating across the EU
- 3) Image viewing – Not suitable to view a 'Screenshot' to declare a match.
- 4) Security of the data and network

Some respondents were in agreement that the database should be a Virtual Database and not centralised. A central database would create noise and there would be some questions about legality. The Virtual Dbase (distributed) would gain more attention locally and the data would be managed more effectively. Other respondents were silent on the issue other than to state their support for the sharing of the information. Some said this was a technical issue beyond their control and understanding. It is recommended that consideration be given to this point and the very real benefits that a distributed network would deliver. From an intelligence management and data exploitation point of view the distributed network would seem to be the best approach and the least invasive although more work is required to test this assumption.

There are a range of different policies in place about the identification of firearms and bullets and cartridge cases, comparison of ballistics materials, storage and retention policies, retrieval of stored data and the production of evidence at court. It is recommended that there is a need to consider harmonisation of forensic processes across the EU and ENFSI could play a part in this. It is Recommended that attention should be paid to the work of J.F. Nijboer and W.J.M. Sprangers 'Harmonisation in Forensic Expertise; An Inquiry Into the desirability of and Opportunities for International Standards'. (Criminal Sciences).

On the issue of information sharing with different Member States the general and overwhelming view was that EU Members are largely already within a federated trust network. However, one said that they would not recommend a sharing of information outside the EU with any other State unless directed to do so.

Many respondents stated that intelligence management was organised around specific crime types. I.e. Intelligence for burglary, for care crime, for robbery, for homicide, sex crimes and so on within their police departments. Comments were received about how they would be interested in learning more about different methods of managing intelligence. It is recommended that this receive attention of the Working Group because there are opportunities for the dissemination of Best Practice.

One respondent had undertaken extensive research and published a paper concerning the operational effectiveness of the IBIS system³ used widely across the EU. This provides a valuable study of the relative effectiveness and the best practice approaches in the use of IBIS. For example, the article demonstrates a 75%-95% success rate for cartridge case analysis and 50%-

³ **A Parameter Study Regarding the IBIS™ Correlator: Nennstiel, Ruprecht; Rahm, Joachim. Journal of Forensic Sciences, Volume 51, Number 1, January 2006, pp. 18-23(6)**

75% for bullets under certain conditions. The important point in this publication is that different patterns of use create different outcomes.

WHY SHARE DATA – THE BENEFITS?

Some respondents raised questions about the benefits of data sharing and how this could provide assistance to the forensic investigation process. These comments were not negative nor did they question the motives for wanting to share information. They simply wanted to know what the benefits were and how they would help solve crime problems. For the purposes of the Report this matter receives attention. It is a core issue for the Proposal.

In the middle of the last century scientists began to examine whether computers could in themselves solve problems that involve the manipulation of data and symbols as well as the management of calculations. In short they wanted to see if computers could act like humans in solving intractable problems.

It is a fact that not all problems can be solved by calculus. The Financial Markets provide the perfect example and there lessons to be learnt from them about complex decision systems. Although the Markets deal with huge numbers of transactions there are inexplicable variables operating that drive the Markets more like a 'swarm of ants' than a body of calculations with fixed states. Teams of humans drive the process by interacting with each other and computers in highly complex relationships and with many different purposes. There are many variables driving the decisions the humans make. This is similar to the problems encountered in decision making in crime investigation and especially in the field of intelligence analysis.

One of the terms used to describe this work was Artificial Intelligence (A.I.). It has however only recently begun to be successful with the arrival and onslaught of powerful computing. An early observation of these scientists was that the systems they used tended to mimic the way humans solve

problems. This was surprising at first because the intention of the programmers was to write the best optimised program for the task. It was discovered that a large part of effective problem solving is determined by the 'problem space' or environment in which the problem is encountered. The complexity of problem solving is inherent in the problem itself rather than in the problem solver. The solving of problems and discovering elements of problems is situational-dependent. The process of solving a problem involves moving ones mind from one state to another in a series of moves over time. Because we don't have a road map of how to solve a new problem we approach it stage by stage, bit by bit and break it down into 'states'. We eventually find the answer but it has taken many iterations and many states to do so. This is serial thinking and it is distinctly different to the parallel style of thinking and systems operation that is proposed by this Report. In serial thinking one thing is dealt with at a time one after the other. There is rarely parallel thinking (or processing) taking place. When humans act in interoperable teams (similar to ants in a swarm) they are able to act in a parallel fashion by marshalling their joint efforts to consider and share experiences of the many attributes of the problem and the environment all at the same time. Humans have become dominant precisely due to this 'team' mentality. Data sharing as proposed by this Report would be another example of this 'team mentality'.

There is a key factor that causes humans to think in a serial way and it is connected with humans short term memory. This major implications in crime investigation and intelligence analysis because we can only retain a small amount of data in our minds at any one time and so we have to move in small serial steps from problem through to solution step by step. Computers can do this extremely quickly and very reliably and they never get tired! Furthermore, computers can exploit parallel processing which accelerates the effectiveness of processing power.

A common strategy for humans is to use the environment or the problem space to look for 'clues' as to how best to go about solving the problem. The environment of the problem we face is therefore critical to solving the problem. This is justification for seeking to change the environment for the management of ballistics information so that we can act in parallel rather than in serial steps as is currently the case.

Crime is a classic problem space issue and this is why it attracts such attention from authors and crime fiction fanatics. It is the essence of environmentally driven problem solving.

Those who 'organise' and use the environment best will inevitably become the best problem solvers. Detection of crime and terrorism is no different. How well we organise the information we have and the environment in which it is managed will dictate how successful we become at using the information to achieve things we need or desire – solving crime.

In order to solve problems we need to be able to note and describe the attributes of the problem AND the problem space AND a series of consequences that may flow from taking different combinations of actions. A good example at this point is to think about the finger-print or firearms examiner searching for correlations and trying to piece together a set of events with explanations (moving from problem towards conclusion setting).

Attributes of problems are measurable or at least capable of being described. Striae on bullets and breach face marks on cartridge cases are observable phenomenon and therefore measurable. As such we can manage them in series of comparisons with other marks to decide whether or not a match or correlation can be declared. The problem is of course that this process is time-consuming and we are liable to lose sight of an attribute due to our short term memory as we progress. However, with enough time and support we can find a match in our collection.

The limiting factors in this scenario is the serial nature of the problem solving process (one step at a time and in consideration of a range of possible outcomes one at a time) and the limited problem space or work environment in which we operate. The stimulus we receive is limited and few suggestions are put to us about the best possible range of outcomes and the problem space environment.

Now consider the same situation of the fingerprint or firearms examiner working in a federated team across a large problem space or environment where there are many opportunities for stimulus (information sharing about attributes) and a multitude of signals about the environment. Imagine this situation supported by computers that do not share the frail short term memory of humans, can process parallel signals and attributes quickly and ***they never forget.*** This is the sort of environment that would exist with a Network Firearms Intelligence Database.

A mistake however is to engage simply in the mass collection of information without building up expertise and techniques in making sense of that information. As well as fast collection devices (grid computers for example) we must have strategies for search, retrieval and analysis that help us solve problems. In short, the process is parallel problem solving facilitated by search, retrieval and enquiry – *not as is often the case namely mass collection and occasional searching.*

THE WHOLE IS WORTH MORE THAN THE SUM OF THE PARTS

One very good thing about mass collections of data and information is that each item of information has an inherent ability to combine in many different ways with any other items of information in the collection. We can thus discover a great deal simply by trying and testing combinations. However, this can cause problems because exponential combinations can occur and we

can produce more combinations than we have the capacity for making sense of.

A combination is the fusion of two or more attributes of data that may correlate or tell a story important to solving a problem. In general, the number of possible combinations of two or more evidence items, when we have n items, is: $2^n - (n+1)$. This amounts to an exponential explosion of information. The potential for complex combinations can be illustrated by a simple example.

If we assume that only 10 items of data (variables) there would be 1013 different ways of combining and assembling them into patterns. If there were 25 variables (for example, simple categories like people, events, locations), there would be 33,554,406 ways of combining and assembling them into interesting combinations. If there were just 50 variables involved, the number would be immense and more than 1.126×10^{15} . That is truly an enormous number and why the whole is worth more than the sum of the parts!

In order to exploit mass collections of data we need intelligent methods of exploiting the ability to compare or combine any item of data with any other item of data. Furthermore, we need a method to help us reduce the massive possible numbers of combinations down to numbers we are capable of dealing with.

Computers can and do play a great role in this function by helping us to grade the sorts of combinations and correlations we would like to make. However, if this is done within a team environment where there is a collective intelligence at play (a Network Firearms Intelligence Database for example) we have the potential to stimulate the system to promote ideas about where to look first and where the most effective strategies might be found to solve the problem.

Simple things like suggestions from colleagues or suggestions from systems generated by routine comparisons of recurring phenomenon, exception analysis, standard-deviations are all examples of routines that can help us make sense of the data. This so much more powerful if it is done within a framework of trust and sharing of information. The possibilities are simply greater and the parallel effort of humans and computers creates the stimulus required for problem solving. This form of 'Group Think' supported by interactive computing (humans and computers working symbiotically together) provides a powerful approach and exceeds the sort of situation often seen in criminal investigation where humans work within limited environments with hard and fast borders to their domain - they are *stifled* rather than *networked* for facts.

Networked systems and parallel working practices of data sharing within the system will allow the investigation team to mount very powerful data-mining and data querying processes way beyond that currently available. They will be able to pursue obvious lines of investigation based on the knowledge they currently have but they will also be able to contemplate less obvious lines of enquiry that may turn out to be fruitful as the process unfolds.

A technical note on this has been provided.⁴ In this (footnote) example we are considering a population of people and a set of crimes as well as

⁴ Consider a set of crimes (a_i) and a set of people (b_j) who could have committed those crimes, where:

a_i = the i^{th} recorded crime, where $i = 1, 2... N(t)$
 b_j = the j^{th} person in the population, where $j = 1, 2... M(t)$
 $N(t)$ = total number of people at time t .

$M(t) =$

Further, let the probability at time t that person b_j is associated with crime a_i , based upon the information available, be $p_{ij}(t)$.

Hence, we know that a useful measure of the uncertainty which exists in the system is given by the entropy which is defined as

$$H(t) = -K \sum_{i=1}^{N(t)} \sum_{j=1}^{M(t)} p_{ij}(t) \log p_{ij}(t)$$

where K is a constant and is dependent upon the choice of units of measure used.

evidence coming to light over time. The calculus demonstrates that the problem is scaleable, measurable and capable of being supported by a computer. This is precisely the situation faced by the firearms examiner using a comparison microscope. The work of this individual is much more scaleable and fruitful within a federated network of data, activity and stimulus.

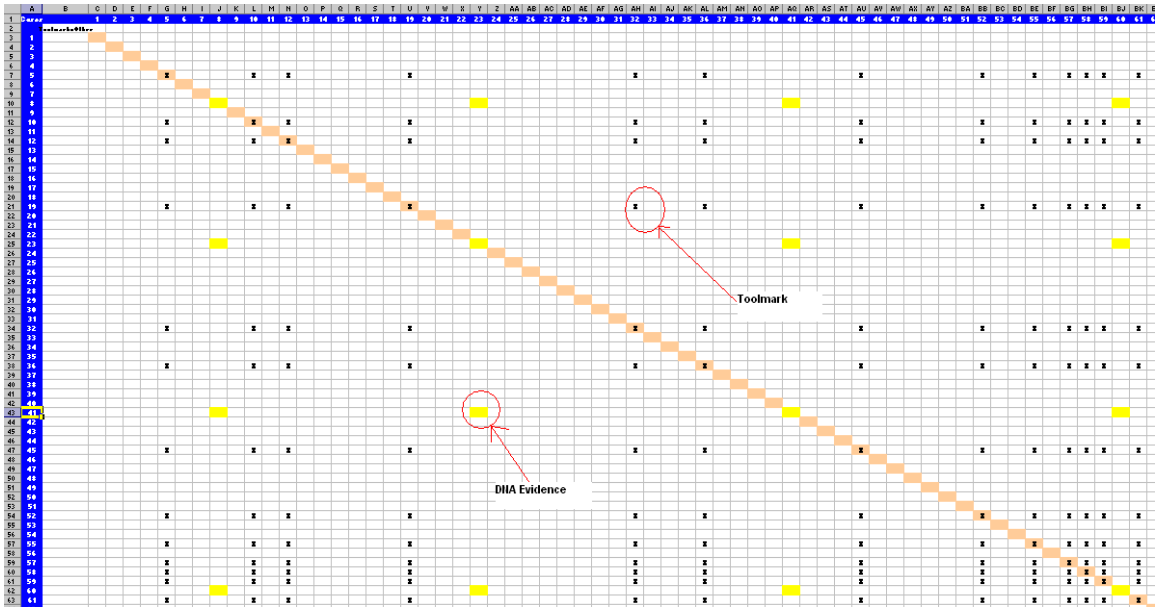
The following illustration demonstrates the immense combinatorial power of the simplest computer available – a *simple Matrix*. In this case crimes are counted along each axis of the Matrix namely 'X' and 'Y' and evidence is added to the Matrix over time as it becomes available. In this example the evidence items are marked with 'X'. It can be readily seen that very quickly we have built a powerful means to manage, collate and never forget where any one item of evidence is and how it connects two or more crimes together. Imagine this Matrix with ten million entries on each 'X' and 'Y' axis and the massive power to store and Report matches. Imagine all EU ballistics information stored in this way. The power for linking would be immense.

Suppose that in the next interval of time, further information is received concerning the number of recorded crimes, the number of people in the population, and the probabilities with which they are associated. Thus, the entropy (uncertainty) level at time (t+1) is given by:

$$H(t+1) = -K \sum_{i=1}^{N(t+1)} \sum_{j=1}^{M(t+1)} p_{ij}(t+1) \log p_{ij}(t+1)$$

This means that if we wish to define the value of this information in terms of the effect it has on the uncertainty of the system, a measure of its value is given by:

$$\blacktriangle H = H(t) - H(t+1)$$



THE PROBLEM OF SECURITY

Whilst there was overall support for the sharing of information many views were expressed about the issue of security of information and networks. This theme was the single most pressing issue of concern. Concerns ranged from security of data, security against intrusion, exploitation of data, identity management and national security issues within Members home States. Comments were made about the need to be able to protect local policy whilst at the same time contribute to the overall security of the EU. There is clearly a need for Member States entering into the use of advanced information sharing systems to become producers of security rather than merely users of security when the need arises. Specific attention needs to be given to these concerns because they may pervade further than the Members of the Working Group.

MANAGING SECURITY

Security is an essential component and feature in modern networked systems especially those dealing with law enforcement information. As well as security of the infrastructure itself a major problem is the ability to implement and maintain an identity management system so that audit systems can operate and access controls be maintained. Access rights and controls for member States is an important feature of this information sharing approach. Access rights and controls and identity management systems and architectures can be used as federated 'Trust Management Systems' and key to the development of the type of system subject of this Report and proposal.

Another concern was interference with ICT architectures sometimes called 'hacking' and information theft. Intrusion Detection Systems (IDS) in security frameworks are now becoming common. This should be treated as an aligned security component to support the 'Trust Management System'. It needs to take account of local and network threats so that the exchange of threat information between disparate environments can take place and enable the Trust Management Systems to react in an aligned effective way.

The boundaries between internal and external information systems are beginning to become less defined in the 21st Century. The traditional approach to security and borders is eroding in favour of the distinct advantages that can be gained from responsibly managed information sharing initiatives. Organisations need to protect their security boundary but they need to open their data and business critical systems to tap into the added value gained from federated information sharing policies.

Organisations like EUROPOL can extend their value add by acting as a 'trusted broker'. The new organisation of the 21st Century is the 'Virtual Organisation' and they are not limited by geographical location. They are not susceptible to the old problems of limited geographical space within which to

work. The move to the so called Virtual Organisation is creating the need for sophisticated security models, ones attainable with federated Trust and Security Management. EUROPOL and law enforcement agencies across the EU will in time become members of these federated 'Trust Management Systems'. The cost of being outside them will in only a short time from now be too much to endure. Being part of the 'whole' in information sharing is being able to share the benefits of more than the sum of the parts.

Within a federated trust and security management system, organisations can work securely with autonomous internal and external strategic business units that locate within a trusted domain inside the enterprise. Third party identity services shared amongst other trusted domains (trusted circle of friends) and across a common and secure enterprise bus enables effective control measures to be employed and maintained.

The use of these 'Trust Management and Security Systems' requires a balancing of legal, regulatory, privacy and security concerns as a precondition for securing and managing the virtual organisation paradigm within a Pan-European ICT spaces. Harmonisation of legal and regulatory frameworks can be achieved through EU legislative bodies most of which currently exist. For example, the first stage of the Pan-European Networked Firearms Intelligence Database need not involve sharing any personal information. The information can be limited to scientific data about contact trace marks and geographic and reference data about crime.

Interpreting security and trust in the context of the EU vision encompassed in ISTAG 2003 Report on Ambient Intelligence⁵ allows a federated trust approach to be taken that contributes to this ambient intelligence notion by

⁵ ISTAG reflects and advises on the definition and implementation of a coherent policy for research in ICT in Europe. This policy should ensure the mastering of technology and its applications, and should help strengthen industrial competitiveness and address the main European societal challenges. This includes crime and security.

allowing interoperability between Grid applications and thereby facilitating ambient driven e-collaboration between organisations. The EU is providing a clear policy view for the use and exploitation of ICT in creating a more inclusive, safe and prosperous EU taking this approach:

“Security-related issues are coming to the fore in a number of policy areas. Border security, protection against **terrorism and crime, transportation security, protection of critical infrastructure, disaster management, and information network security** are all areas demanding new security-focused solutions. At the same time, in the search for higher levels of protection for its citizens, Europe must defend its commitment to a democratic, pluralist, open and liberal society. Striking the right balance between security and freedom will be a permanent challenge. ICT is crucial to these developments, in particular in providing the interoperability and connectivity to enable systems to work across different authorities and countries. Europe needs to act quickly if it is to remain at the forefront of technology research, and for industry to meet the rapidly emerging needs for sophisticated security-related products and services”.⁶

Management of electronic identity within the same federated EU wide computing infrastructure will be a significant challenge. Therefore, security considerations to prohibit identity theft, intrusion and theft of data necessitates fundamental security policies.

To solve these unsolved problems, the system will need to address the following objectives:

1. A framework for federated Trust and Security Management as an enabling architecture.
2. Secure Information Systems; Those that Member States using heterogeneous EU computing infrastructures consider to be trustworthy.
3. A secure Identity Management System where Global Virtual Identities for both organisations and individuals operate.

⁶ Shaping the Future Through ICT: ISTAG Report 2006.

4. Interoperability amongst disparate ICT implementations to meet authentication and authorisation requirements within the 'Trust Management System'.

In implementing the proposals of this Project it will be necessary to satisfying these requirements and clearly address:

1. Protection of data and privacy.
2. Intrusion prevention and detection.
3. Identity management, and confirmation
4. Identity theft prevention.
5. Organisational Privacy and Confidentiality,
6. Trust and trust relationship management

Secure authentication is an essential requirement and 'credential management' a crucial component of the identity management system. Services will be required that create secure access sessions for applications and services across enterprise boundaries and Member States.

Policy requirements will be needed to allow a standard secure approach to express and make available the application and services and the security policies under which these will run in. For example, if an additional trust relationship exists with another party (the concept of a circle of trust) then what types of credentials, requests and privacy policies are acceptable?

The immediate features of such a security approach would be the following:

- Single Sign On; One secure authentication
- Only policy approved information is passed to the federated network across the EU (the ICT Service)

- Satisfaction that the security and usage policies defined are enforced locally and across the network

The significance and importance of security to Members of the Homicide Working Group cannot be overstated but these should not be allowed to overshadow the many benefits that Members of the Homicide Working Group have identified. Digital authentication, authorisation, privacy and trust are all well understood issues in ICT in 2007 and need to be underpinned with security protocols that will need to be defined. The following are key issues needed to satisfy Members of the Homicide Working Group:

- Define a secure architecture for a federated identity management system for services working in a disparate environment;
- Incorporate the framework architecture into the existing services, supporting backwards compatibility and bottom up systems;
- Establish a Federated Global Virtual Identity Management Policy
- Establish a policy and technology for Trust Management
- Establish a policy and technology for Intrusion Detection
- Integrate existing identity and security solutions in EU network technologies (meeting global ICT standards).

There is a problem of incompatibility of disparate Member security infrastructures in relation to both the data format and policy. When adopting a Virtual Organisations (VO) or infrastructure approach there is a need to obtain an identity certificate in the format specific to the infrastructure concerned locally and across the network. This will necessitate going through the certification process which is specific to the organisation owning the resource.

A Federated Trust and Security Management System has the potential to solve these problems by providing open standards and protocols with the ability to span and move between different Virtual Organisations and infrastructures. Members will need to operate within an environment of cooperation and trust of joint users and services but with the ability to

control their access points and levels of data sharing. Some may wish to have their policies managed by themselves alone to increase the security. Whilst this may slow down interoperability and data sharing it will encourage levels of trust to grow and flourish over time. It is a fact that the deployment of a federated identity infrastructure limits an organisations vulnerability to security attacks overall because there are more gate-keepers with greater access to greater amounts of security related information about potential threats. The organisation as a whole grows and with it confidence and trust.

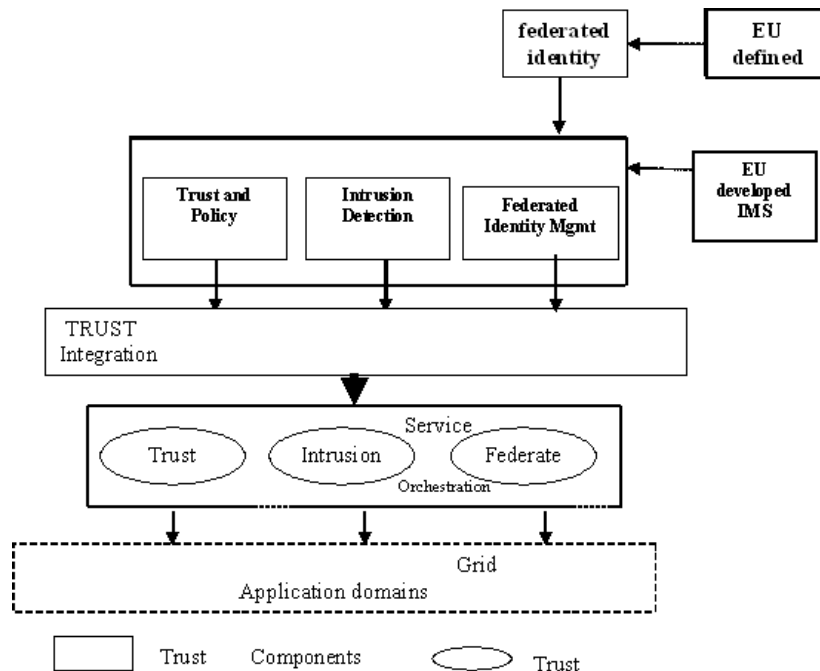
The increased levels of security required and the reduction of serious crime and terrorism across the EU necessitate increased sharing of information between Member States. This therefore impacts upon the importance of security to ensure that the benefits of sharing data are safeguarded. A federated identity approach for users and managers could provide single all-encompassing security standard for Member State to Member State applications that encourages mutual confidence and trust between them when sharing information. The benefits will bring economies of scale, cost savings, operational efficiencies, and increased security to all in ensuring crime is detected quickly and on a bigger scale than has previously been the case. A spin off benefit will be an acceptance of networked data sharing technologies by law enforcement across the EU as grid technology is greatly enhanced. Those EU Member States that grasp the concept of information sharing in ballistic evidence and intelligence in the way foreseen will have a greater chance to gain security and safety for the public they serve.

The benefits of implementing a federated network for information sharing supported by a Trust Management System and identity strategy and infrastructure are as follows:

- Better use of intelligence for security and risk management;
- Enhanced coalitions with neighbours and beyond through interoperability and information sharing;

- Best Value and cost effectiveness, cost reduction. All through increased operational efficiencies due to faster response times for critical information exchanges;
- Growth through development of joint gains and strategic sharing and offerings of information.

The following diagram outlines the nature of the Federated Trust Management System and the identity Management Certification model:



This model would be applied across the entire system to put in place a Federated Trust Management System.

Richard M Leary
Forensic Pathways
March 2007

APPENDICES

APPENDIX 1

**The European Commission Directorate-General Justice and Home Affairs
(AGIS Project – European Networked Firearms Intelligence Database)**

European Country Member _____

Interviewee _____

Interviewer _____

Other Persons Present _____

Signatures:

Interviewee _____

Interviewer _____

Date Form Completed _____

**The European Commission Directorate-General Justice and Home Affairs
(AGIS Project – European Networked Firearms Intelligence Database)**

11. On the basis of your knowledge about crime and forensic investigational policy, and the possible benefits that might accrue, please indicate which countries of the European Union, your government would be interested in sharing criminal ballistic technical data with:

- | | |
|---|--|
| <input type="checkbox"/> Austria | <input type="checkbox"/> Belgium |
| <input type="checkbox"/> Cyprus | <input type="checkbox"/> Czech Republic |
| <input type="checkbox"/> Denmark | <input type="checkbox"/> Estonia |
| <input type="checkbox"/> Germany | <input type="checkbox"/> Greece |
| <input type="checkbox"/> Finland | <input type="checkbox"/> France |
| <input type="checkbox"/> Hungary | <input type="checkbox"/> Ireland |
| <input type="checkbox"/> Italy | <input type="checkbox"/> Latvia |
| <input type="checkbox"/> Lithuania | <input type="checkbox"/> Luxembourg |
| <input type="checkbox"/> Malta | <input type="checkbox"/> Poland |
| <input type="checkbox"/> Portugal | <input type="checkbox"/> Slovakia |
| <input type="checkbox"/> Slovenia | <input type="checkbox"/> Spain |
| <input type="checkbox"/> Sweden | <input type="checkbox"/> The Netherlands |
| <input type="checkbox"/> United Kingdom | |

**The European Commission Directorate-General Justice and Home Affairs
(AGIS Project – European Networked Firearms Intelligence Database)**

- 12. On the basis of your knowledge about crime and forensic investigational policy, and the possible benefits that might accrue, please indicate which other IBIS countries your government would be interested in sharing criminal ballistic technical data for investigative purposes:**

| | | |
|-------------------|----------------|---------------------------|
| _____USA | _____Kosovo | _____Chile |
| _____Canada | _____Brazil | _____Venezuela |
| _____Turkey | _____Australia | _____Trinidad & Tobago |
| _____Algeria | _____Kenya | _____Mexico |
| _____Israel | _____India | _____South Africa |
| _____Thailand | _____Russia | _____Hong Kong |
| _____Saudi Arabia | _____Colombia | |

**Thank you for your co-operation in the completion
of this questionnaire.**

APPENDIX 2

FIGURE 1

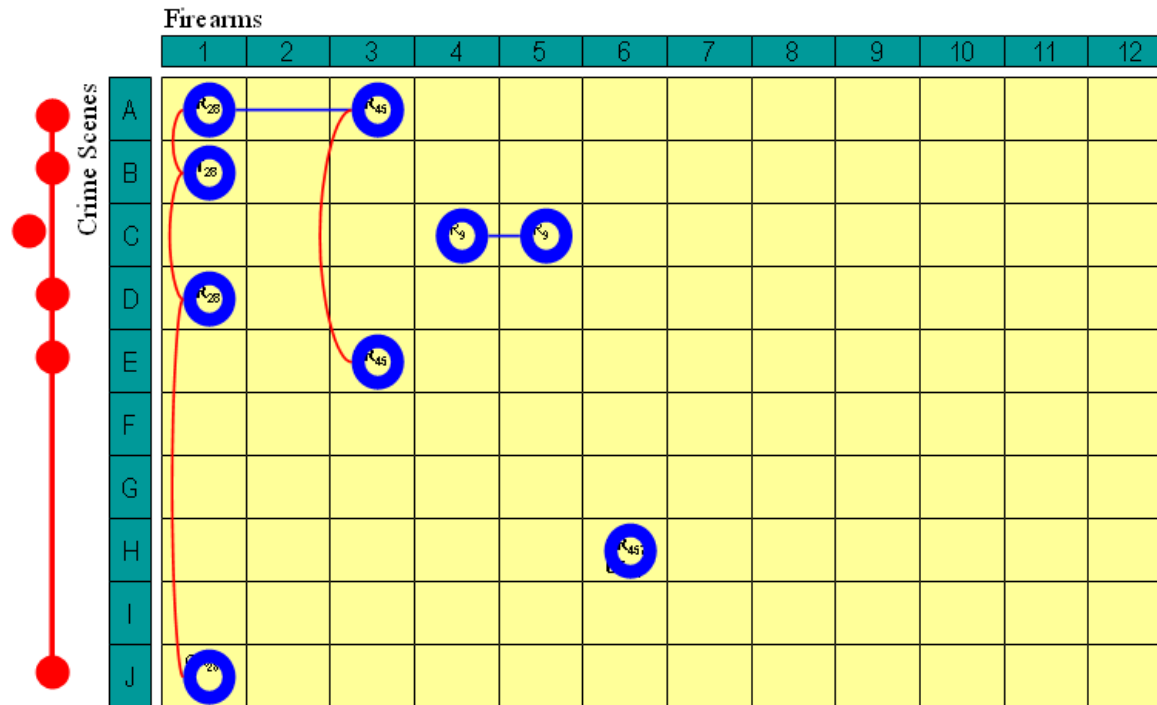
What Data Sharing Can Do For Gun Crime Advanced Linking

| | | Firearms | | | | | | | | | | | |
|--------------|---|------------------|---|------------------|-----------------|-----------------|--|---|---|---|----|----|----|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Crime Scenes | A | CR ₂₈ | | CR ₄₅ | | | | | | | | | |
| | B | CT ₂₈ | | | | | | | | | | | |
| | C | | | | CR ₉ | CR ₉ | | | | | | | |
| | D | CR ₂₈ | | | | | | | | | | | |
| | E | | | CR ₄₅ | | | | | | | | | |
| | F | | | | | | | | | | | | |
| | G | | | | | | | | | | | | |
| | H | | | | | | CR ₄₅₇ CT ₄₅₇ | | | | | | |
| | I | | | | | | | | | | | | |
| | J | CR ₂₈ | | | | | | | | | | | |

Figure 1 shows the Matrix and the ballistics evidence all in place.

FIGURE 2

Adding The Ballistics Data To The Matrix



In Figure 2 the same Matrix shows the ballistics evidence added to the Matrix. The red lines and dots denote linked Crime Scenes.

FIGURE 3

Diagram of Links Between Ammunition, Test Fired Weapons and Crimes

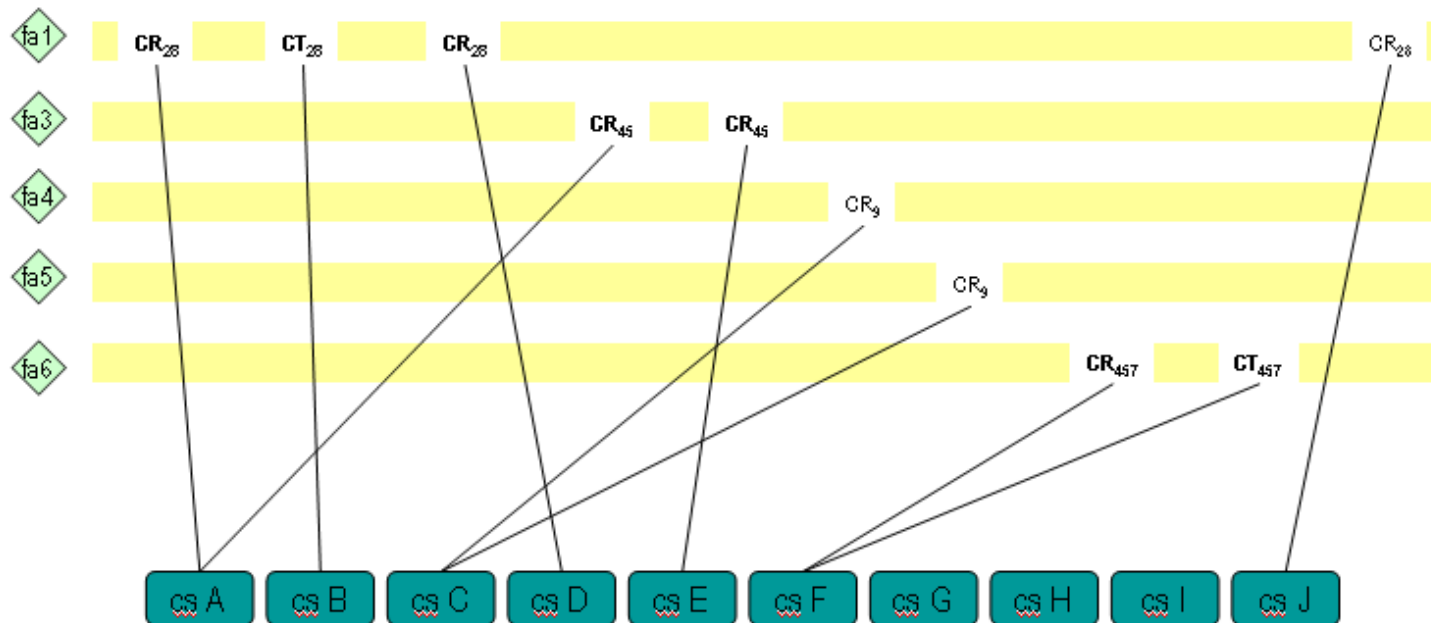


Figure 3 shows how the Crime entities are linked to the evidence types and the evidence are linked to crime and firearms.

FIGURE 4

Firearm “Identities”

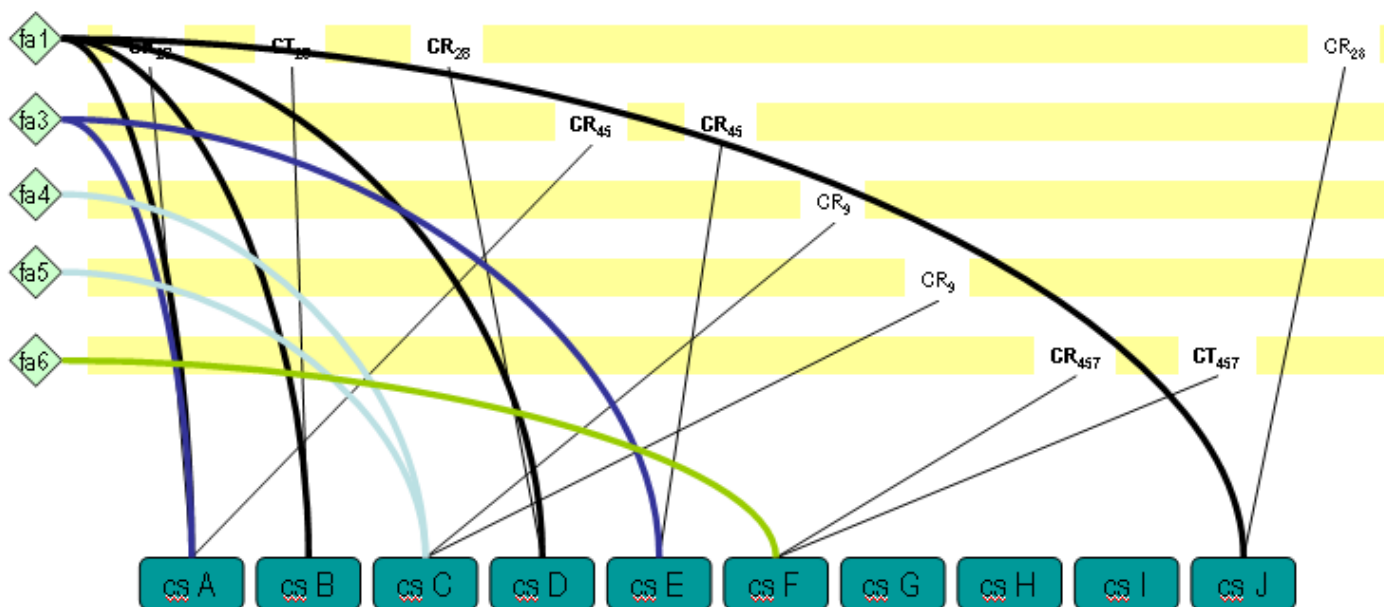


Figure 4 illustrates the links to firearms and their resulting identities.

FIGURE 5

Links Identified - Step 1

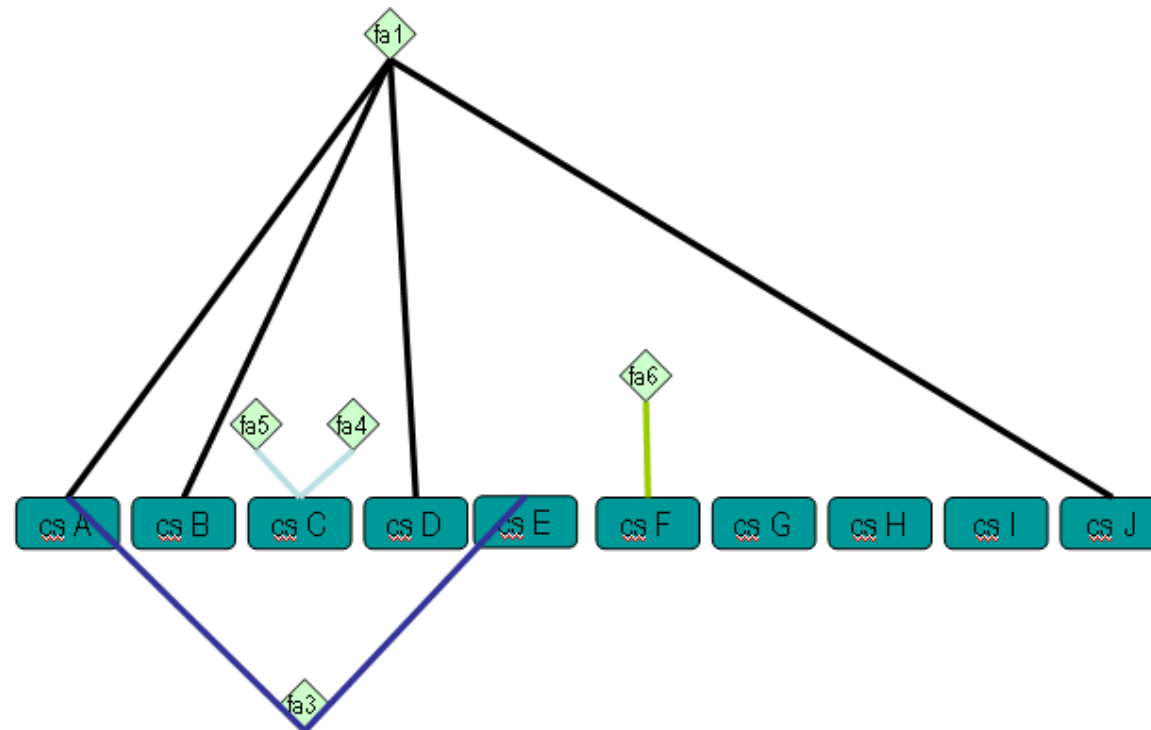


FIGURE 6

Links Identified – Step 2

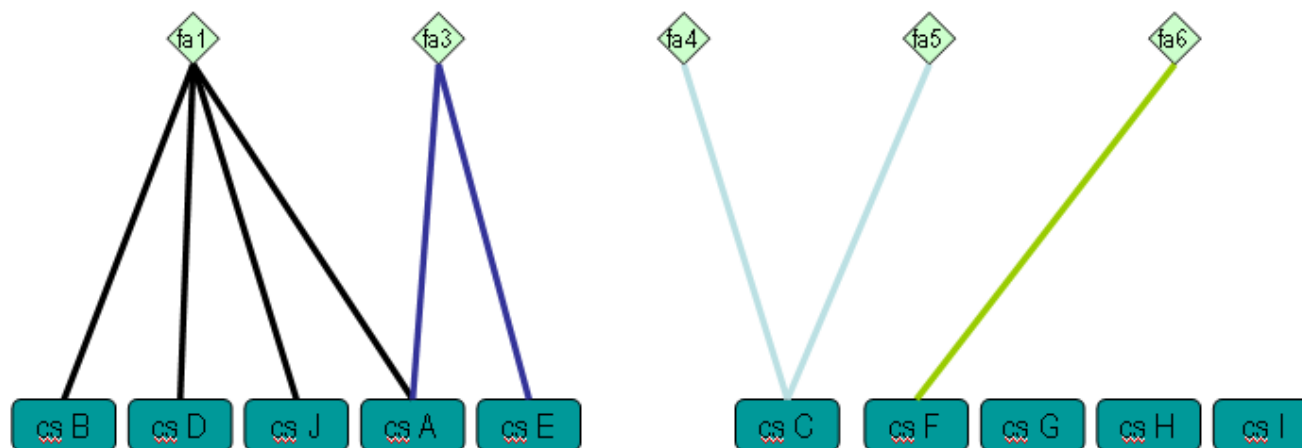


Figure 6 illustrates linked crime in a number of series.

FIGURE 7

Adding Suspects

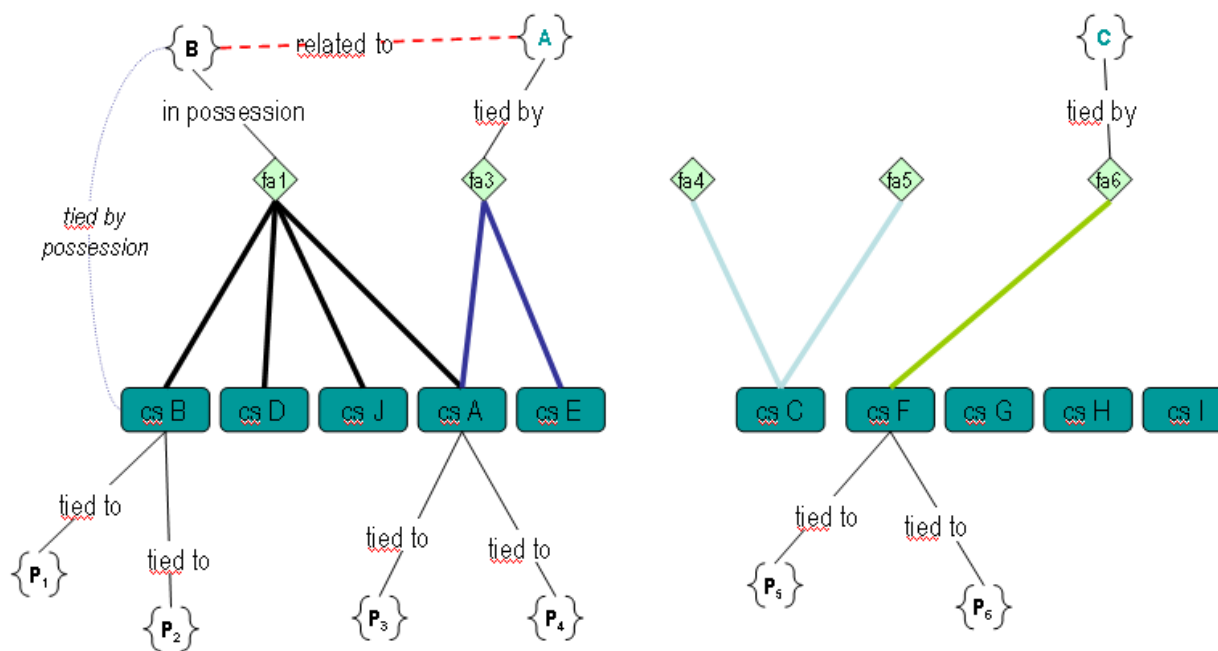


Figure 7 shows 'suspects' added to the Chart and their links.

FIGURE 8

The Case Builds

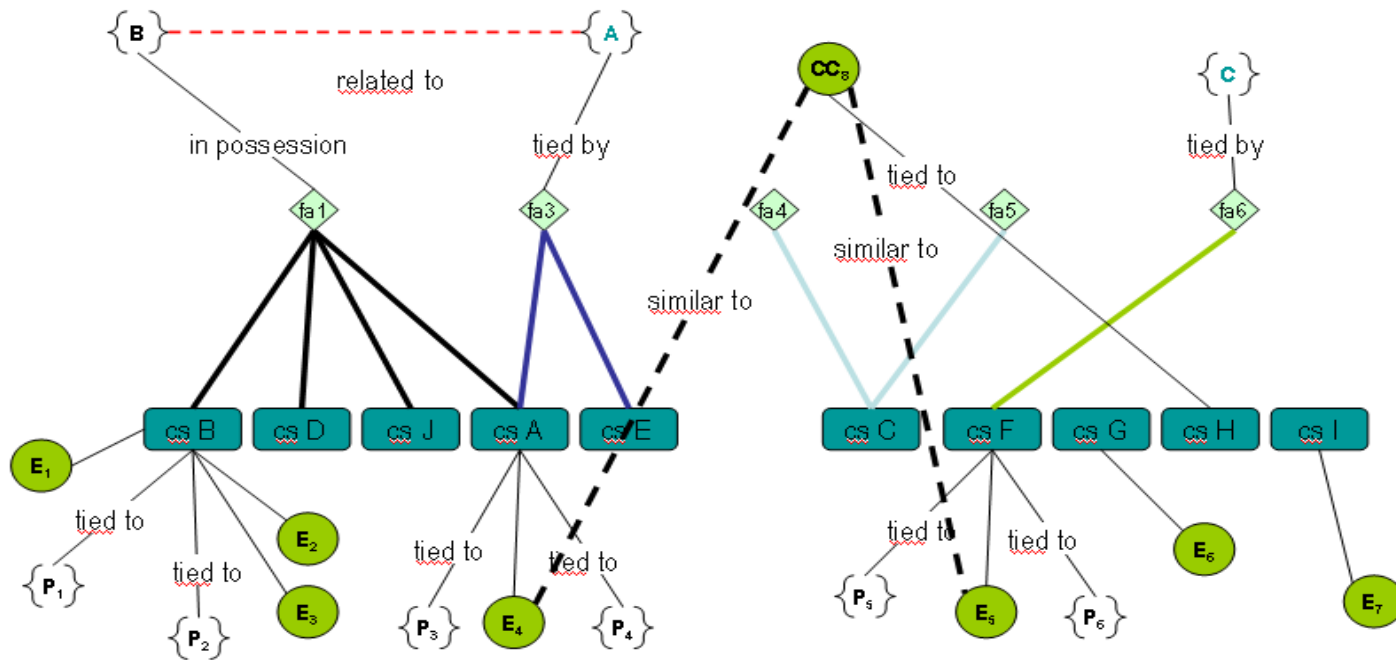


FIGURE 9

Ultimate Proposition – Case As a Whole

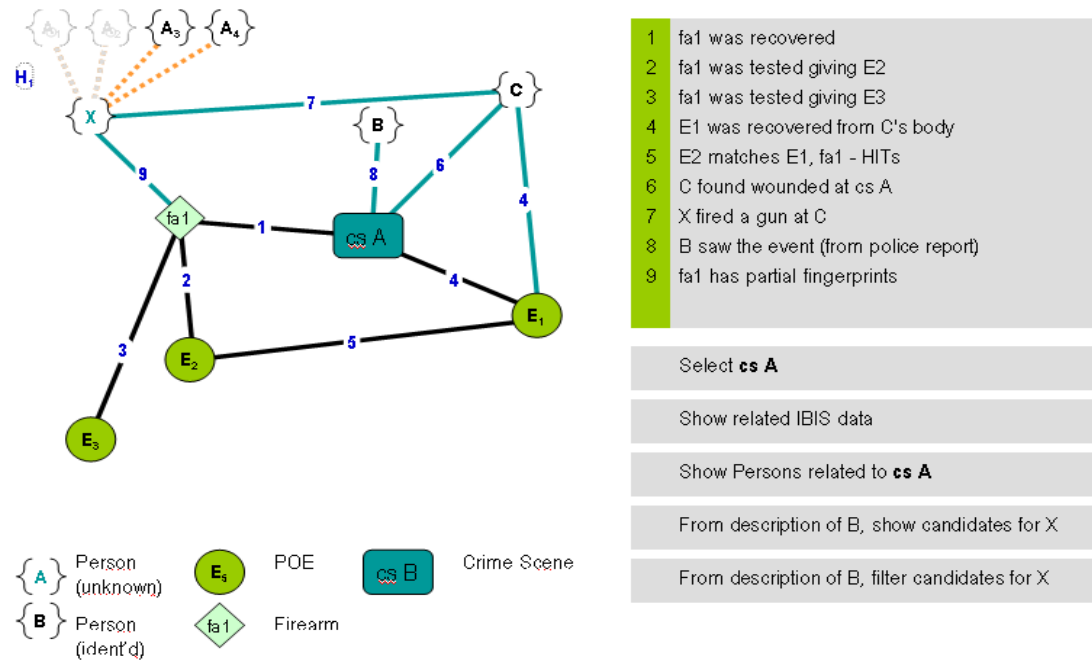


Figure 9 illustrates the ballistics evidence as a whole to the man,

SCHEDULE

EU Ballistics Intelligence Trust Management System

EU Ballistics Intelligence Trust Management System:

| | |
|---|---|
| <p>AIMS</p> <p><u>Better Use Of Intelligence</u> <u>Interoperability And Information Sharing;</u> <u>Best Value</u> <u>Growth AND Added Value</u> <u>Protection of data & Privacy</u> <u>Intrusion protection</u> <u>Identity management</u> <u>Identity theft prevention</u> <u>Organisation privacy & confidentiality</u> <u>Trust management</u></p> | <ol style="list-style-type: none"> 1. Better use of intelligence for security and risk management; 2. Enhanced coalitions with neighbours and beyond through interoperability and information sharing; 3. Best Value and Cost Effectiveness, Cost Reduction. All through increased operational efficiencies due to faster response times for critical information exchanges; 4. Growth and added value through development of joint gains and strategic sharing and offerings of information; 5. Protection of data and privacy; 6. Intrusion prevention and detection; 7. Identity management, and confirmation; 8. Identity theft prevention; 9. Organisational Privacy and Confidentiality; 10. Trust and trust relationship management. |
| <p>MANAGED SECURITY - REQUIREMENTS DEFINITION:</p> <p><u>Federated Identity Management</u> <u>Backwards Compatibility</u> <u>Federated Global Virtual Identity Management</u> <u>Policy – Trust Management</u> <u>Policy – Intrusion Detection</u> <u>Integration – Existing Security</u></p> | <ol style="list-style-type: none"> 1. Define a secure architecture for a federated identity management system for services working in a disparate environment; 2. Incorporate the framework architecture into the existing services, supporting backwards compatibility and bottom up systems; 3. Establish a Federated Global Virtual Identity Management Policy; 4. Establish policy and technology for Trust Management; 5. Establish policy and technology for Intrusion Detection; 6. Integrate existing identity and security solutions in EU network technologies (meeting global ICT standards). |

| | |
|--|---|
| <p>EU LEGAL FRAMEWORK LEGAL PRINCIPLES COVERING THE SHARING OF DATA FOR THE EUROPEAN BALLISTICS INTELLIGENCE SYSTEM</p> <p><u>Scientific Information</u> <u>Crime Information</u> <u>National Law</u> <u>Eu Law</u> <u>Policies</u> <u>Gun Registration Schemes</u> <u>EU Legal Framework</u></p> | <ol style="list-style-type: none"> 1. Identify available technical and <u>scientific information</u> for each Member State (non-personal); 2. Identify available relevant <u>crime information</u> in each Member State (non-personal); 3. Identify relevant <u>National law</u> relating to sharing technical intelligence for each Member State; 4. Identify relevant <u>EU law</u> relating to sharing technical intelligence; 5. Define <u>policies</u> in each Member State relating to sharing technical intelligence; 6. Identify EU Member States with <u>Gun Registration Schemes</u> – legally and voluntary based; 7. Develop White Paper on current <u>EU legal framework</u> for project. |
| <p>DATA ACQUISITION PROCESS</p> <p><u>Comparison Microscopes</u> <u>Databases</u> <u>Data</u> <u>Format</u> <u>Quantity</u> <u>Timescale</u> <u>Storage & Weeding</u> <u>Software in Use</u> <u>Data Acquisition Process</u></p> | <ol style="list-style-type: none"> 1. Identify all Ballistics Comparison Microscopes and Data Acquisition Platforms in use in Member States (Regardless of Brand); 2. Identify databases storing ballistics information in Member States (Regardless of Brand) 3. Data available; 4. Data Format; 5. Quantity of data available; 6. Timescale over which data collected to-date (scale); 7. Identify storage method, location, and weeding time limits on storage; 8. Identify databases and any software applications used to collect and manage data; 9. Develop strategic data acquisition process. |

| | |
|---|---|
| <p>DEFINE SECURITY PROBLEMS TO BE ADDRESSED</p> <p><u>Federated Trust And Security Management</u> <u>Computing Infrastructures</u> <u>Secure Identity Management</u> <u>Interoperability Amongst Disparate ICT Platforms</u> <u>Authentication And Authorisation</u> <u>Security Levels</u> <u>Strategic Model</u> <u>Security Infrastructure</u></p> | <ol style="list-style-type: none"> 1. A framework for federated Trust and Security Management as an enabling architecture for the project; 2. Establish requirements for Secure Information System with trustworthy heterogeneous EU computing infrastructures; 3. Establish requirements for Secure Identity Management System where Global Virtual Identities for both organisations and staff operate; 4. Establish requirements for Interoperability amongst disparate ICT implementations to meet authentication and authorisation requirements within the ‘Trust Management System’; 5. Define security levels for each Member State; 6. Define strategic model of combined security levels; 7. Define <i>Security Infrastructure</i> to deliver on Trust Management System. |
| <p>ACCESS AUTHORITY</p> <p><u>Agencies Authorized Access Levels</u> <u>Agencies Authorized To Investigate</u> <u>Agencies Authorized To Prosecute</u> <u>Authorized To Allow Evidence Exchange</u> <u>Specific Authorisations</u> <u>Proof Required In Criminal Cases</u></p> | <ol style="list-style-type: none"> 1. Establish Agencies authorized to have access to the data; 2. Establish Agencies authorized to investigate; 3. Establish Agencies authorized to prosecute; 4. Establish Agencies authorized to allow evidence exchange requests and sanction same; 5. Establish what specific authorisations are there available; 6. Establish level of proof required in criminal cases to declare a match, if so, what and by Member State. |

| | |
|--|---|
| <p>DATA INTEGRATION AND QUERYING FOR INTELLIGENCE REQUIREMENTS</p> <p><u>'Specific User Requirements'</u> <u>Intelligence Products And Services</u> <u>'Europol User Requirements'</u> <u>Strategic Requirements</u> <u>Correlations For Tactical And Strategic Intelligence Requirements</u> <u>Query Processing Engine</u> <u>Fixed Query Management And Model-Based Querying</u> <u>Optimisation Issues</u></p> | <p><u>USER REQUIREMENTS</u></p> <ol style="list-style-type: none"> 1. Identify '<u>Specific User Requirements</u>' of each Member State regarding their own required level of <u>intelligence products and services</u> – <i>What, who, when, why, how do users need to know;</i> 2. Identify 'EUROPOL User Requirements' regarding <u>intelligence products and services</u> – <i>What, who, when, why, how do users need to know;</i> 3. Identify joint strategic requirements bearing in mind 1 and 2; 4. Identify the most important correlations for tactical and strategic intelligence requirements; 5. Identify requirements for query processing engine - fixed query management and model-based querying approach; 6. Identify modeling requirements. <p><u>OPTIMISATION</u></p> <ol style="list-style-type: none"> 7. Identify optimum technical methods for data acquisition; 8. Identify optimum technical methods for data sharing and access; 9. Identify optimum technical methods for QUERYING; 10. Develop strategic integration plan; 11. Identify optimum approach for distributed querying methods. |
| <p>PERFORMANCE MEASURES</p> <p><u>Standards and Performance</u></p> | <ol style="list-style-type: none"> 1. Standards and performance monitoring and evaluation requirements of each Member State currently; 2. Standards and performance monitoring and evaluation requirements of each Member State in future. |

SELECTED BIBLIOGRAPHY

1. Brady Campaign to Prevent Gun Violence. Statement by Sarah Brady on the sniper shootings [news release]. 2002 Oct 8 (<http://www.bradycampaign.org>).
2. AA Braga and GL Pierce: Assessing the Value Added to Gun Law Enforcement Operations by IBIS Technology
3. Braga A, Kennedy D, Waring E, Piehl, A. Problem-oriented policing, deterrence, and youth violence: An evaluation of Boston's Operation Ceasefire. *J Res Crim Delinq* 2001;38:195–225.
4. Campbell DT, Stanley J. Experimental and quasi-experimental designs for research. Chicago: Rand McNally, 1966.
5. Cook T, Campbell D. Quasi-experimentation: Design and analysis issues for field settings. Boston: Houghton Mifflin, 1979.
6. De Kinder, J. Review AB1717 Report. Technical evaluation: Feasibility of a ballistics imaging database for all new handgun sales. Brussels, Belgium: National Institute for Forensic Science, 2002.
7. Dr Jan De Kinder, Ballistics Section, Head National Institute for Forensic Science (NICC/INCC), Brussels, Belgium. Technical Evaluation: Feasibility of a Ballistics Imaging Database for All New Handgun Sales.
8. Gardner W, Mulvey EP, Shaw EC. Regression analyses of counts and rates: Poisson, overdispersed Poisson, and negative binomial models. *Psychol. Bull* 1995;118:392–404. [PubMed]
9. King G. Event count models for international relations: Generalizations and applications. *Int Stud Q* 1989;33:123–47.

10. Kopel DB, Burnett HS. Ballistics imaging: Not ready for prime time. Dallas, TX: National Center for Policy Analysis, 2003. Policy Backgrounder, No. 160.
11. Kleck G. Targeting guns: Firearms and their control. New York: Aldine de Gruyter, 1997.
12. Linking Crime Guns: The Impact of Ballistics Imaging Technology on the Productivity of the Boston Police Department's Ballistics Unit – Authorised reprint from Journal of Forensic Sciences, July 2004.
13. Long JS. Regression models for categorical and limited dependent variables. Thousand Oaks, CA: Sage Publications, 1997.
14. McDowall D, McCleary R, Meidinger E, Hay R. Interrupted time series analysis. Newbury Park, CA: Sage Publications, 1980.
15. Murphy SP. Police say detective was killed by gun found in vacant lot. The Boston Globe 1993 Oct 9; Sect. Metro/region: 17(col. 4).
16. Overcoming Barriers to the Efficient Processing of Evidence Associated with Firearm-related Crime – Forensic Technology 2004.
17. StataCorp. Stata statistical software: Release 7.0. Reference H-P. College Station, TX: Stata Corporation, 2001.
18. The Methods and Technology for "Ballistic Fingerprinting" and Their Practical Applications – Forensic Technology, January 2001, Second Edition.
19. Thompson RM, Miller J, Ols MG, Budden JC. Ballistics imaging and comparison of crime gun evidence by the Bureau of Alcohol, Tobacco, and Firearms. Washington, DC: U.S. Department of the Treasury, 2002.

20. Tulleners FA. Technical evaluation of a ballistics imaging database for all new handgun sales. Sacramento, CA: California Department of Justice, 2001.
21. U.S. Bureau of Alcohol, Tobacco, and Firearms (ATF). The missing link: Ballistics technology that helps solve crimes. Washington, DC: U.S. Bureau of Alcohol, Tobacco, and Firearms, 2001.
22. J.F. Nijboer and W.J.M. Sprangers 'Harmonisation in Forensic Expertise; An Inquiry Into the desirability of and Opportunities for International Standards'. Thela Thesis (Criminal Sciences).