Chapter XVI

Semiotic Analysis of E-Policing Strategies in the United Kingdom

Kecheng Liu, The University of Reading, UK

Michael Hu, The Police IT Organisation, UK


Abstract

Technological infrastructure must satisfy business requirements, and more importantly, it must be able to evolve to meet the new requirements. This requires not only a good understanding of business strategies, visions and functions, but also the evolvability built into the architecture. This chapter first presents a semiotic approach to the business and information technology (hereafter IT) systems. This approach treats the IT system as an integral part of the business organisation. The chapter then discusses the applicability of a semiotic framework in the e-government in the UK, particularly in an evolvable architecture for e-policing. The semiotic framework is applied in the assessment of the e-government strategies and systems requirements, and in the analysis of these requirements to the e-architecture. A case study demonstrating the applicability of the framework is conducted to evaluate the implementation of the national Information Systems Strategy for the Police Service (ISS4PS) and the Crime Justice Information Technology community (CJIT) in the UK.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Introduction

Three categories of e-government applications can be identified (Marchionini et al., 2003): access to information, transaction services and citizen participation, each of which represents a stage of the development history of e-government.

In the United Kingdom, the e-government initiative is underpinned by the UK government appointing in 2001 its e-envoy, who reports directly to the Prime Minister. The e-envoy's office has three core objectives: 1) to make all government services available electronically by 2005, with key services achieving high levels of use; 2) to ensure that everyone who wants Internet access has it by 2005; and 3) to develop the UK as a world leader for business. As the first step, the most popular government services will be made available online as soon as possible, to allow more efficient access through the Internet to the information available in different statuary bodies and ministries, as well as different government agencies/organisations. This will be followed by transaction services and citizen participation including services to business, benefits and personal taxation, transport information and booking, education, health, citizen interactions with the justice system, land and property, agriculture, and e-democracy (BCS, 2003).

Drawing experience from e-commerce and e-business from industry, the advocates of e-government agree that the aims of e-government should not be cost saving, but other more profound benefits. PCIP (2002) has suggested a list of possible reasons and goals for e-government:

- Improving services to citizens;
- Improving the productivity (and efficiency) of government agencies;
- Strengthening the legal system and law enforcement;
- Promoting priority economic sectors;
- Improving the quality of life for disadvantaged communities; and
- Strengthening good governance and broadening public participation.

This list represents the vision of most governments and organisations in most countries. In a study by SOCITM (2003a) conducted in the 441 local authorities in England, Wales and Scotland (over 230 councils took part and responded to the survey), it shows that is an optimism within councils about e-government to deliver better services to citizens, with service improvements forecast at 100% in some areas and an average of 20% across all services. Local authority spending on information and communication technology is forecast to rise by 25% to almost £2.5 billion this fiscal year. However, the success of e-government will reply on multiple factors: appropriate telecommunication infrastructure, business process re-engineering, integration of IT and business processes, citizen participation, readiness of government staff, officials' readiness for change, and many more. Amongst all these, human and organisational factors are more crucial than technological aspects. Successful examples of e-government, experience and best practice, particularly in small councils, are disseminated by SOCITM (2003b) for others to share.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

As an important part of the e-government initiative in the UK, the e-policing programme is introduced to revolutionise the Police Service and improve the effectiveness of crime prevention and detection, by providing the following (PITO, 2002).

- ready access for the public to the police information and services through a variety of easy to use, safe and secure channels, including the use of intermediaries;
- provision of information and services of relevance to the citizen, particularly victims of crime, in a timely and efficient manner;
- support for joined-up working across police forces and with other criminal justice agencies and local authorities;
- better use of information across all forces and with other criminal justice agencies to support the implementation of the National Intelligence Model and to make policing more effective in combating criminality;
- the collection, exchange and storage of information in a secure and trusted environment;
- flexibility to accommodate new business requirements and to take advantage of changes in technology.

Implementing and rolling out the e-policing programme demands an extension of the traditional police service with the more efficient, more transparent, and more citizen-centred business process and underlying technical infrastructure. This requires the change of culture and business processes that have been in place for crime reporting, intelligence gathering, crime analysis, command and control, and many other parts of the business; it also requires an integrated and modernised police IT systems deployed in the business in parallel to the national systems re-engineering and modernisation programmes to the police IT systems throughout the country. In this chapter, an approach for co-design for business and IT systems will be presented. The theoretical framework derived will be used in the assessment of business and IT strategies for e-policing, one of key e-government initiatives the UK.

Background

Historically, more than 50 police forces in UK independently developed their own IT systems to support their work, which, although guided by principles defined by the Home Office, has resulted in separate systems with different structures and functions. These IT systems, usually initially developed in 1980s, are based on dated technologies; some are still running on the terminal-mainframe platform. The Police National Computer (PNC), launched in 1977, provides the police forces with key information needed for crime investigation, usually via direct terminal access. Now an important question is how to deal with these legacy systems to meet the new business requirements in police and criminal justice systems.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

PITO, the Police Information Technology Organisation, as a non-departmental public body was established in 1997, and acquired its statutory status in 1998, with the UK British Home Office as its sponsor department. The organisation's remit includes England, Wales and Scotland. PITO provides information technology and communications systems and services to the police and other criminal justice organisations within the United Kingdom. Recognising that "information and communication technology (ICT) capabilities play a key role in meeting the Government's objectives and the Home Secretary's priorities for policing" (PITO, 2003), PITO has been leading the strategic planning and implementation of organisational and technological infrastructure for e-policing. One of the important items on PITO's agenda is re-engineering and migration of the legacy police information systems to a web-enabled platform which supports the online police information exchange and processing, and enables the revolutionary concept of e-policing.

An Organisational Semiotic Approach

The co-design of business and IT systems is an approach towards the development of the two systems in a flexible and adaptable manner (Liu et al., 2002). Within an organisation, the deployment of information technology does not change the business nature, but only the way the business is conducted. This lends to a holistic view of two parts (business and IT systems) being interrelated. Following the Organisational Semiotics (Stamper et al., 1988; Liu, 2000; Liu et al., 2001), a business organisation is by and large a system of information and communication. This is because in the organisations, information is created, stored, and processed for communication and coordination and for achieving the organisational objectives. In some organisations, information processing may be the core business, such as in service industry, for example, banking, insurance and consultancy. In this type of industry, information and services are their products. In other organisations, information processing and communication is to support the production of physical goods and other substantive activities. To a large extent, e-government involves a great deal of the first type of activities, which produce information. An IT system should be viewed as an integral part of the business organisation; the design of both the IT and business systems must be conducted simultaneously. The organic integration of IT into the business processes will allow both systems to evolve naturally.

An organisation, as an integrated business and IT system, can be seen as an architecture having multiple layers, three of which constitute the technical infrastructure:

- *physical* devices and their interconnections - the computer hardware, the network, the optical fibres, the satellites, and so forth, which generate and carry a cause-and-effect chain of events quickly and cheaply, across the globe if necessary;
- *signalling* protocols, the validation, authentication and encryption routines that exploit the basic physical phenomena, so that a varied stream of patterns originat-

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

ing in one place can be reproduced, ideally without error, at another place, or corrected in case of error;

- *structures* that enable signals to be combined into messages, to be analysed into parts (parsed), stored in files, retrieved, used in calculations, and recombined into new messages.

The design, implementation and maintenance of these three layers are the tasks of the IT department, whose responsibilities are to make sure these technical components are functional and adequate to support business operations.

Other three layers in the system architecture are perhaps more important in conducting the business:

- meanings of the numbers, words and expressions that form a message, and the ways that meanings combine to create the meaning of the message as a whole;
- communicating the intentions of the message, through interaction and negotiation between appropriate actors;
- social consequence in the form of established commitment, obligation and responsibly between the people involved.

All these are close to the core business issues that are related to the business objectives of police operations.

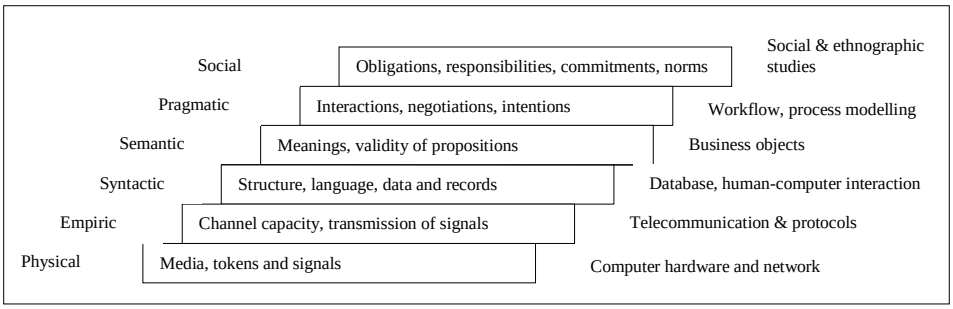
Adopting Stamper's Semiotic Framework (Stamper, 1996), we can summarise the above key issues of an IT embedded system at the six semiotic levels (Figure 1). On the left of the diagram suitable names for the levels are given; the key issues are mentioned in the middle; and, on the right are listed the solutions available or approaches to be attempted.

We shall develop the organisational system with IT component at all these levels, but at the technical levels, our solutions are distinguished by being formal and precise. The physical level solutions are implemented in the form of interconnecting networks of standardised telecommunication devices and computers. We can be almost certain when these are correctly established and when they break down; thus the quality of the physical systems can be assured. At the empiric level we use various standard communication protocols (such as PC/TIP) to exploit the physical devices. These take care of encoding, switching, error detection and correction, the confirmation of transmission and so forth. They, like the physical standards, are established globally. The syntactic level is also formal and precise but here it is more difficult to establish global standards. Great efforts in industry have been made to bring in standard forms of communications in computer and information technology, for example SOAP and UDDI in Web services. Some standards have been established but it is difficult to agree on global solutions and the standards tend to be modified at the local level according to the business norms of the industry.

The problems at the upper three layers are less studied and difficult to find "standard" solutions, though organisational semiotics places a great emphasis on them. The problems at the semantic level can be explained by the need to encapsulate meanings of

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Figure 1: Key issues of Internet based systems analysed using the Semiotic Framework



communication within the message syntax solutions, which is commonly acknowledged as the most difficult task. The representation of intentions and social obligations by any IT system is more of a challenge that many systems development methods would not consider, although the semiotic approach (Liu, 2000) has offered mechanisms and techniques whose benefits have been increasingly recognised. Semiotic methods have been applied in examining how information is used in virtual and distributed organisations to enhance the competitiveness (De Moor, 2002; Gazendam, 2001, 2002). Industrial applications have also been carried out in requirements engineering and process modelling for e-policing (e.g., Xie et al., 2003).

Systems Requirements and Architecture for E-Policing

PITO, as a national organisation responsible for IT policies and strategies for the UK police forces, has set up many task forces to look into different issues, including the IT infrastructure and functionality of the e-policing systems. As a result of the investigation, it has emerged that the environment for the future e-policing should include:

- Information from all police and criminal justice (CJ) organisations that is up-to-date, of known provenance and readily available for use at the point of decision-making
- Enhancement on data and information sharing among the police forces and national agencies, and between the police and other CJ partners
- The capacity for a co-ordinated response across force boundaries using the intelligence generated from multiple information sources
- Greater capability to tackle serious and major crime
- More direct, efficient, and interactive interfaces between the police and public
- Common standardised business processes to harness "best of breed" police systems that support those ACPO (Association of Chief Police Officers) endorsed business processes

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- A business information framework that points the way to reuse such systems (as software components) at minimum cost within other forces and/or complex processes
- A common minimum standard for the technical infrastructure, with advancements planned and co-ordinated
- Solutions to address local, regional and national business problems as appropriate.

Many current initiatives have been driven by immediate business needs. For example, the online vehicle number plate enquiry enables the cruising police officer to check the vehicle details on the road. On top of all these, we believe a more thorough understanding of the police work will lead to significant changes in the manner and quality of services. Understanding of the police business processes will be the basis for embedding the Web enabled technologies into the daily workflow of the police forces, which will provide a solid foundation for the e-policing strategies and implementations.

PITO has been tasked to lead the national programme of implementing and rolling-out the e-policing in UK. The principal strategic/business driver for such a programme is to make all government services (with exclusions for policy or operational reasons) available electronically by 2005 as set by the UK government (e-envoy's office paper at www.e-envoy.gov.uk).

It is important for the police service to plan the provision of electronic facilities for the range of communications expected from citizens as an alternative to the traditional face-to-face contact. In addition to the improved accessibility to police services, other factors in the modernising government agenda are of importance for e-policing:

- building services around citizen choices;
- providing for social inclusion; and
- making better use of information.

Thus, any new facilities brought in as part of e-policing, wherever possible, should be focused on the citizen rather than being designed around the sole needs of the police. E-policing must help the police to make better use within and between forces of the information in their possession to combat criminality.

Whilst the operational aspects of the police response to these strategic drivers will be through local forces, because of the federated nature of the police service, a common and joined-up approach in the way that central government envisages is likely to be achieved only by a corporate response and co-ordinated strategy.

Current Infrastructure

There exists a well-established and fairly efficient business process in the police service in UK that has been in application in the 53 police services throughout the country. This

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

is supported by an underlying technical infrastructure that is developed in the last three decades, including

- A portfolio of core IT systems used in the police forces;
- A substantial data repository in the Police National Computer (PNC);
- A backbone of secure communication network.

A wide range of IT systems have been developed in the last several decades in the 43 police forces in England and Wales (not counting in Scotland), serving thousands of on-duty police officers throughout the UK as well as the Criminal Justice System (CJS) community. Many of these systems are currently being upgraded with added functionality, while new systems are continuously being developed and rolled out. The backbone of IT systems to support policing nationwide is the Police National Computer (PNC), which has been in service for 30 years. Over the years, the system has grown to embrace many technological advances, incorporating advice from the government and policing bodies, as well as from in-house and industry technical experts. It has developed from a record keeping service to a sophisticated intelligence tool. It holds extensive data on criminals, vehicles and property, which is accessible in a matter of seconds, through more than 10,000 terminals in police forces across the country (PITO, 2003).

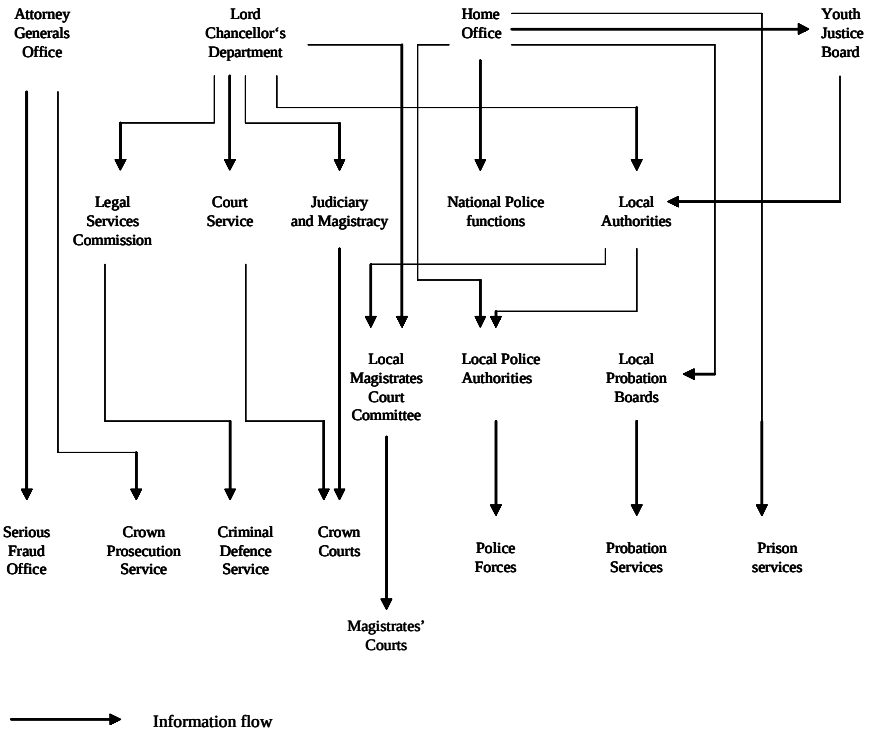
The police IT systems and PNC are connected via the Police National Network Communications that link all police forces, the Home Office and other criminal justice organisations.

Whilst the police/public interface had improved through the introduction of the Police Portal and in some areas "one stop shops," there is no formally agreed upon strategy to ensure the development and delivery of a coherent programme. Common facilities across the service will only succeed if supported by the introduction of standard business processes. There is a slow adoption of best practice in individual forces, and little central promulgation of best practice and little overall programme management function to drive the business process improvements forward. More generally, there is only limited interoperability and integration between systems within forces and a low level of data sharing between forces and with other criminal justice agencies. This impacts on the forces' abilities to make best use of the valuable data held throughout the service. While interfacing and business process improvement may be seen as part of the overall information systems strategy or contained within other programmes of work, the Police/Public Interface programme set the goals to improve these interfaces to deliver all the benefits of e-policing.

There is also little coordination of approach to common services such as security and presentation of information. A wide range of interfaces to core systems exist, as there are no service-wide standards to follow and a plethora of local applications operating in individual forces. As there is no mandate for forces to adopt common systems and standards, there is an inconsistent approach and the potential for duplication of effort is enormous. Data quality is variable between forces. These factors impact on the service's ability to present a "joined-up" appearance and cannot be regarded as cost-effective nor provide best value.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Figure 2: Information shared amongst the key members of the CJS



Many of the initiatives in PITO are in the form of studies or pilot projects. There is a danger that the strong messages to come out of these may not be disseminated to forces or embraced by the wider police service partly because of the absence of an overall strategy and programme management function. Moreover, with the police service as one of the key members of the criminal justice system (CJS), it is within PITO's remit to enable a full integration between the police IT systems and other parts of the CJS, so that a seamless collaboration is achieved. Figure 2 shows the key member organisations within the CJS and how information is shared between them (Parsons-Hann, 2003).

Business and Systems Requirements

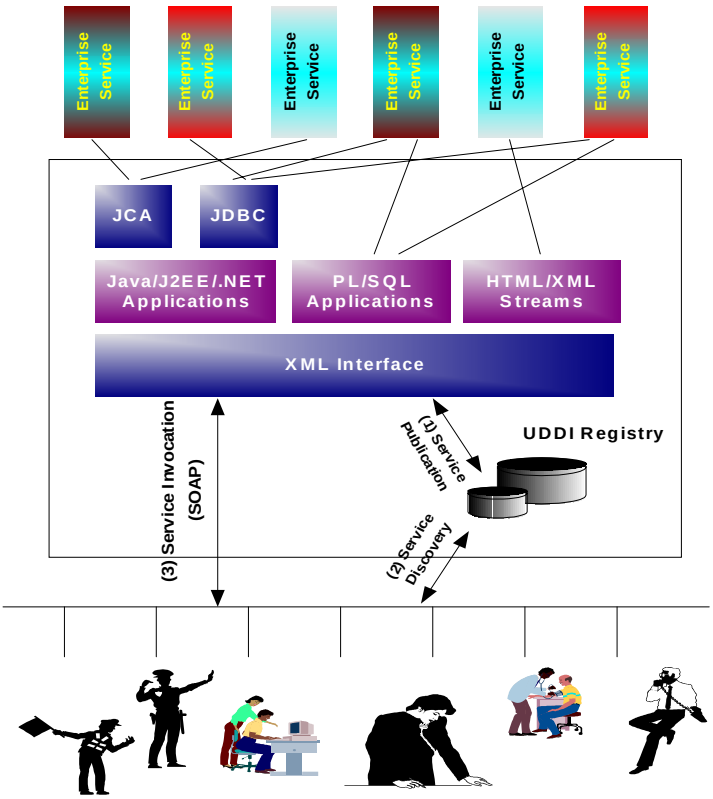
Business targets in several business areas have been identified for the next few years (*ww.pito.org.uk/what_we_do*):

- Communications: This target is to achieve clear and secure voice and data communication, as it is vital to any successful police operation. This area is important because officers rely on it for their safety and that of their colleagues.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- Criminal Justice: All police information systems must be able to share information with other CJS systems. Access to the police systems will be provided to CJS agencies. Information and communications technology holds the key to joining together criminal justice organisations and improving the way they work together.
- Identification: The ability to identify "one person from many" is a fundamental concept in policing. Technology now enables the police to do this more quickly and accurately than ever.
- Intelligence and Investigation: Successful police operations need to be founded on reliable intelligence and sound investigative practice. Collating that intelligence, sharing it with police colleagues and giving them the tools to unlock its potential are key aims in this area.
- Police National Computer: The PNC is an unparalleled source of police intelligence available to all forces nationwide. Steady infrastructure upgrade and the addition of new databases have been implemented to make sure the PNC continues meeting the police needs.
- Police Support Services: Improving police efficiency and effectiveness is not all about front line policing. Forces need IT applications that help them to report and analyse performance and get the most out of the resources they have available.

Figure 3: The police services information systems architecture



Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Whilst the definition of e-policing at first glance could include the whole spectrum of policing, it is appropriate to focus the initial e-policing programme on the police/public interface as that must be delivered electronically by 2005 to meet the government's targets. This will build on the current Police/Public Interface programme and is consistent with the agreed scope of the police service information systems strategy (code name Valiant) as shown diagrammatically in Figure 3. A number of core systems are listed for illustrative purposes only and not all potential channels for public access are depicted.

For the police/public interface (PPI) to be effective, there is a requirement for the scope of e-policing programme to include interconnection to those back-office or legacy systems necessary to achieve the vision. The scope will also extend to include areas of data warehousing to make effective use of the information held in core systems. Apart from the necessary links to back-office systems, all other police core business systems and systems serving staff are considered to be outside the current scope of e-policing. Also, whilst e-policing depends on the Criminal Justice Extranet (CJX) for its delivery, the provision and operation of this network is to be considered outside the scope of the initial e-policing programme

In the long run, police information systems in the UK will go through the modernisation and transformation process, as specified by the national Information System Strategy (as seen in Valiant document 2002). The modernised systems will provide ubiquitous access for the police forces and officers. The capability of knowledge-based processing is also required to support effective policing and collaboration between the police and the CJS organisations.

Case Study: Analysis of the E-Policing Strategies

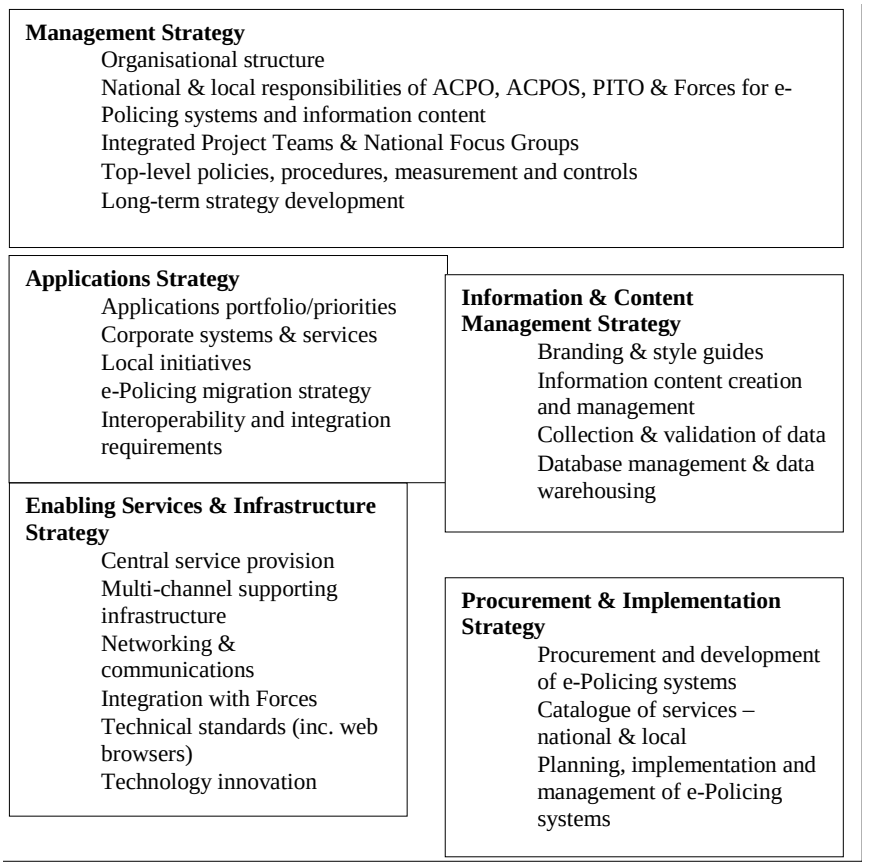
In this section, the Semiotic Framework (see Figure 1) will be used to evaluate the design and implementation of IT infrastructure for e-policing.

To meet the requirements for e-policing, PITO has developed a strategic framework (PITO, 2002) to address the challenges of organisational and technological issues, and the management of expectations and the implementation of infrastructure. The strategic framework for e-policing illustrated in Figure 4 comprises five component strategic areas:

- Governance and Management Strategy
- Applications Strategy
- Enabling Services and Infrastructure Strategy
- Procurement and Implementation Strategy; and
- Information and Content Management Strategy.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Figure 4: The e-policing strategic framework



This framework summarises all the important aspects of the current practice of design and implementation of organisational and technological infrastructure for e-policing. An analysis based on organisational semiotics will enable us to evaluate the e-policing framework by examining the methodological underpinnings.

Governance and Management Strategy - The Social Aspect

In the planning and implementation of IT infrastructure, governmental requirements and police organisations' commitments to the UK society have been seen as the fundamentals. The Governance and Management Strategy covers the following:

- organisational structure to support e-policing
- top-level policies, procedures and controls

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- development of the long-term strategies for e-policing; and
- responsibilities of different government agencies and each individual force in e-policing.

A Semiotic Analysis

As suggested by the semiotic framework, the design of any information systems infrastructure must start from definition of responsibilities, obligations and commitments. The e-policing strategic framework is consistent with this theory by putting the governance and management strategy as the fundamentals. E-policing requires full collaboration between police forces and other criminal justice services. Technologies deployed are only part of the infrastructure, but coordination and collaboration between all organisations involved is more essential in a functional e-policing infrastructure. Guided by the top-level policies and definition of responsibilities, collaborative work processes between agencies, institutions and forces will build an organisational foundation, while modern technologies can enhance the collaborative e-policing.

Applications Strategy - The Pragmatic Aspect

To meet the vision for e-policing, the single biggest challenge is to move from a police-based system development environment to a citizen-centric business model. In the traditional model, the office of Central Customer acts on behalf of police forces by establishing the service requirements and priorities for development. The focus of e-policing on the police/public interface necessitates an extension of this role to capture also the expectations of the citizen.

In the first instance, the developments will be prioritised based on the recent consultation exercise with all forces and ratified by the Central Customer and the EPMG team. PITO will continue to manage the central programme portfolio including systems, services, infrastructure and common practices. Some systems and services within the central e-policing programme portfolio will be provided locally by forces.

The applications strategy will be developed to include:

- strategy for e-policing corporate systems and services, and local initiatives;
- e-policing migration strategy; and
- specification of interoperability and integration requirements to meet the long-term e-policing strategy.

A key issue is the determination of what should be provided centrally and what may be considered at the local level. The proposed strategy for systems and services to be provided centrally will be based on the premise that these provide:

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- corporate single points of contact for the public to engage electronically with the police service; or
- e-policing systems and services that are generic to the police service as a whole and may be replicated across force boundaries.

The e-policing business process model is shown in Figure 5. The citizen expectations, as seen in the model, are the fundamentals to determine the criteria for technical and service performance. These criteria are then applied to the measurement of current services, systems, practices and infrastructure.

A Semiotic Analysis

The applications strategy covers the issues identified in the pragmatic aspect. It takes into account the different perspectives of the various stakeholders and aims at achieving effectiveness of the integrated systems. The strategy considers how the systems and services interact with the citizens as well as other users (i.e., police officers and CJS staff). Measuring the systems and services will lead to identification of possible gaps between what is expected and what is available with the current infrastructure, which may lead to identification of further improvements and solutions to reduce the gaps.

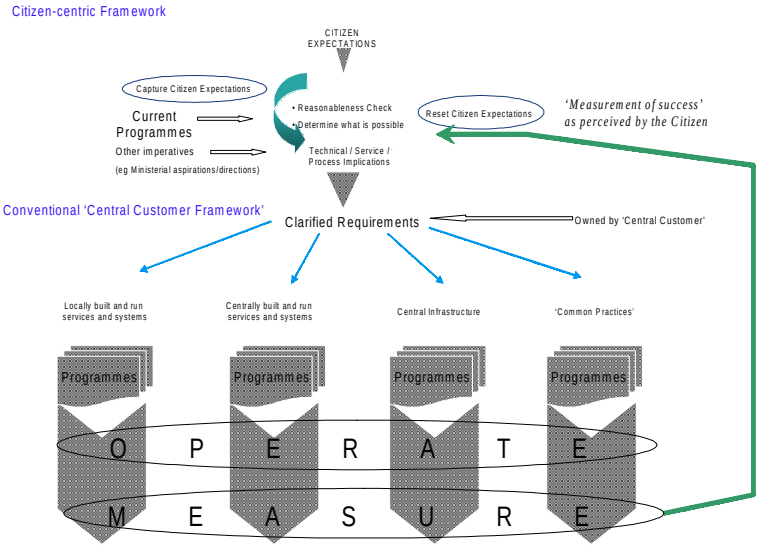
Information and Content Management Strategy - The Semantic Aspect

An overall strategy for the management of data submitted by citizens, and the provision and updating of published information will be developed. This strategy will be provided to the forces as a "toolkit" to ensure a generic framework is used in information and content management throughout the forces. For the majority of the projects within the PPI programme, the information and content management will be the responsibility of forces following policies and procedures issued by the Association of Chief Police Officers and Association of Chief Police Officers of Scotland (ACPO/ACPOS) and the EPMG team within PITO. Part of the planning, design and training for each project will focus on this important area.

The strategy will focus on the branding of police service Web sites and other electronic display facilities so that the public can gain assurance of the ownership of the information and the security of the communication channels used. Other aspects of content and information management will also be covered in this strategy, including responsibility for the collection and validation of data through e-policing channels, database management and data warehousing as it affects e-policing, and the creation and management of the content published electronically by the police service.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Figure 5: An e-policing business process model



A Semiotic Analysis

The information and content management strategy addresses the issues at the semantic level. Information content, meaning and validity are essence for all systems that provide information and services, as described in the semiotic framework. Information should be provided timely and shared by relevant stakeholders. The quality of information provision impacts directly on the quality of police services through e-policing. As shown by experience in many information systems development projects, the semantics of information presents the most challenges, as it is difficult to capture in information models and to represent in information systems. Effective methods for dealing with information semantics have to be identified and deployed in the implementation of e-policing infrastructure.

Enabling Services and Infrastructure Strategy - The Syntactic and Empiric Aspects

In order that the public may be encouraged to use the police portal and other channels in providing often sensitive information to the police and for the police service to make better use of information in its possession in combating criminality, a suitable resilient multi-channel supporting infrastructure is to be provided

The strategy to be developed for enabling services and infrastructure is a key component in the delivery of trusted, secure and joined-up e-policing services. It will include strategies for:

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- provision of central services (e.g., Web hosting, common directories);
- communications infrastructure to support multiple channels (e.g., channel strategy);
- integration with local force infrastructures (e.g., browser interface standards).

A backbone communications infrastructure, CJX, is in place linking all forces and the police portal will be connected to it. This will ensure secure routing of data traffic and the ability for forces to share information. Forces will be responsible for compliance with data protection legislation, conformance to system security policies and the observance of the Government Protective Marking Scheme. The accreditation of other criminal justice agencies to use CJX will continue to be the responsibility of ACPO. The requirement for and viability of adopting the replacement government-wide secure communications network being delivered under GSISP, as the principal communication network for the police service or connecting CJX to it, will be assessed centrally at the appropriate time.

Whilst the strategy is being developed, additional features will be provided through the police portal and the forces will become more dependent on it. As it is supporting operational policing, rigorous testing of new features will be necessary prior to their introduction in a live environment and resiliency will be introduced to ensure its continuous availability.

PITO is well placed to provide information and guidance to forces wishing to link their systems into the e-policing infrastructure. There are a series of national focus groups already in existence, which will be used to review elements of this framework to accommodate e-policing as a priority covering policy/role issues across a range of topics. For example, guidance notes will be provided to cover:

- security elements to be considered across all channels;
- technical and architectural standards to be adopted;
- infrastructure installed to provide the recommended functionality to be used;
- standards for interfaces to back office legacy systems (e.g., Web browsers);
- performance measures and targets for the fulfilment of citizen enquiries and commitments made;
- business process standards (e.g., call centre procedures and practices, data quality, data validation, data cleansing);
- presentation standards for police Web sites (e.g., branding, image, style guides);
- protection of information and codes of practice.

In the longer term, the whole premise, in line with modernising government, will be to provide choices. There is no desire to limit public use of any channel to access e-policing services. A national channel strategy will be developed and it is the intention to provide choices for the public in being able to access police services through a range of channels, including:

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

- the police portal;
- Internet Web sites;
- one stop shops;
- kiosks;
- call centres;
- digital telephony including text messaging;
- intermediaries (e.g., local authority staff); and
- face-to-face contact (e.g., at police stations).

It is important to develop and maintain coherence between the channels so that an individual may choose to use different channels (e.g., Internet to report a minor crime, telephone to report additional information and SMS text messaging to enquire about progress) while the police officer responding is made fully aware of all the information received to date through all channels. This is a central feature of commercial call centre and client relationship models and has important reference value for the integration with back-office systems.

E-policing services delivered through the police portal will continue to be provided centrally but the content for specific features will be requested to be provided and maintained locally. The use of Internet Web sites by forces is to be encouraged to provide information and discrete services better handled at local level. Consideration will be given to the provision of a national Web hosting service, and to standardising the appearance and the function of force Web sites. It is our intention to recommend a form of branding to enhance the appreciation of the police service as a whole and to provide guidance on the overall appearance and functional content of the Web sites. Links through to force Web sites will be provided on the police portal and vice versa.

It may be appropriate for one-stop shops, kiosks and call centres to be operated on a joint agency basis and the use of intermediaries will be encouraged where it is to the advantage of both parties (e.g., abandoned vehicles, noise nuisance), does not compromise security and is likely to provide a higher level of service to the public (e.g., rural areas). Forces will determine locally with partners the most effective and efficient method of providing these facilities.

The provision of conventional face-to-face contact and telephone services locally will be supplemented by a shared non-emergency telephone number, if proven by the concept demonstrator. Calls will be routed to the local force for response. Additionally, the provision of a single number for text messaging is being considered and is at an early stage of investigation. In the long-term, to ensure that e-policing is citizen-centric, all channels will be supplemented by strong links with back-office systems. Due to the disparate nature of these legacy systems, local forces have to provide interfaces with systems that have been developed in-house.

The key decisions required concern the extent to which e-policing in the long-term moves towards a fully functional customer relationship management (CRM) environment. This will determine the extent of the citizen focus provided, the integration required with back-office systems and the data warehousing facilities needed. CRM implies potential

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

intelligence gathering opportunities and we need to be aware of the implications of this, particularly with regard to the customer relationship. Assuming that full citizen-centric capability is required, the integration strategy will provide a road map for the two-stage migration from the current CJX-connected forces to:

a. limited interoperability with back-office systems in forces as required for the first phase of e-policing; and
b. full integration of core systems, data warehousing and e-policing applications as envisaged in the Police Service Information Systems Strategy (Valiant).

It is recognised that for many years forces will be at different stages on the migration towards the fully integrated solution. The integration strategy will be developed as part of ACPO Information Systems Strategy and the need to cater for the diversity of local infrastructures and systems, together with the expectation that different elements of the police community will migrate at different speeds to the centrally provided infrastructure.

A Semiotic Analysis

The enabling services and infrastructure strategy covers the issues of the syntactic and empiric aspects. It defines standards for data structure, information exchange, communication between systems, and interfacing between application layers and back office or legacy systems. Channels for accessing police services and information sources are also defined; for example, the police portal, Internet Web sites, call centres and digital message exchanges. The appropriate syntactic and empiric setting provides the necessary basis for the correct representation of semantics.

Procurement and Implementation Strategy - The Physical Aspect

PITO will take responsibility for the implementation of centrally provided and managed projects within the overall e-policing PPI programme. Forces will be expected to provide project management for local implementations and initiatives. During implementation, business continuity will be a priority and the migration to new systems will be achieved in a manner commensurate with maintaining operational capability at all times. PITO will assist the forces in training for new systems and will provide support to local initiatives taking consideration of the fact that forces will be at different stages in their adoption of e-policing techniques.

A Semiotic Analysis

The procurement and implementation strategy is concerned with the physical aspect of the e-policing infrastructure. PITO has deliberately allowed freedom for the individual

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

forces to choose their own hardware platforms, as long as the syntactical and empiric standards are reinforced, which enables the correct representation and interpretation of information semantics. This separation between the physical platforms from the rest of the aspects in the semiotic framework maximises the flexibility for systems changes. As witnessed in many cases, the need for systems changes arises from both the changes in business requirements and technologies available. The separation between the hardware platforms and other aspects of the e-policing infrastructure will enable the whole set of integrated systems evolve with minimal unnecessary interruption to the rest.

Summary and Future Work

One important initiative similar to e-policing in the USA is COPLINK (Chen et al., 2003). COPLINK recognises the problems that most local police have database systems used by their own personnel, and lack an efficient mechanism for sharing with other forces and agencies. To enhance the national and local police forces' ability to handle massive amounts of information and improve the efficiency of policing, COPLINK sets the target of developing an integrated information and knowledge management environment for capturing, accessing, analysing, visualising and sharing low enforcement related information. Researchers at Virginia Tech and Purdue University, teamed up with Indiana's Family and Social Services Administration (FSSA), have been developing a WebDG infrastructure for e-government (Medjahed et al., 2003).

In our work, input has been drawn from research work of other going e-government and e-policing projects such as US CJIT and Intelligence Service, Dutch Police and Belgium Police, which we shall continue to benefit from.

This chapter presents only a part of the work currently undertaken in PITO of which the second author is responsible for the architectural design. In this chapter, we introduced an organisational semiotic approach to information systems design and implementation. A business organisation is comprised of people and technology. People are teamed up in a certain structure, with defined responsibilities and governed by the norms (rules and regulations). From the perspective of organisational semiotics, these organisations produce and consume information, and therefore are information systems. The organisational as well as technological components of such information systems have to be co-designed together, so that technologies are best fit into the workflows and business processes. The semiotic framework offers an effective guideline in analysing and designing information systems by carefully examining the issues at the six semiotic levels.

PITO, as an organisation responsible for UK's IT strategies, policies and advice on IT systems implementation, has been playing an important role in organisational and technological infrastructure for e-policing in the UK. The e-policing infrastructure will be built on the existing work by all police forces and CJS agencies. Coordination and collaboration between police forces and CJS agencies are required more than before, which is the prerequisite for a successful implementation of e-policing. The research of the current state of the work shows a firm foundation is available in the UK amongst the

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

police forces and CJS services but much more work is needed before an integrated infrastructure is brought into place. The PITO e-policing strategic framework presents the direction for all the working parties involved in the implementation of the e-policing infrastructure.

A semiotic analysis has been performed on the e-policing strategic framework with a view to assess the e-policing strategies. It shows that the e-policing strategic framework covers well the entire range of the semiotic framework. Careful considerations have been given in the e-policing framework to the social, pragmatic, semantic, syntactic, empiric and physical aspects, as suggested in the theory of organisational semiotics. This has given us much confidence about the current work. Our analysis also suggests that semantics of information is, though its importance is recognised, difficult to capture in the information models and systems. The work we have presented here is an analysis of the current practice in the planning and implementation of e-policing infrastructure after the majority of the work has been completed by PITO. It could be more beneficial if organisational semiotics could have been applied earlier. In further work, semiotic methods, such as semantic analysis and other methods for analysing organisational and technical infrastructure, will be considered for detailed planning and implementation of e-policing infrastructure.

E-government involves a large group of stakeholders: government and non-government, service providers and users from all sectors of the society. The key "product" and "commodity" is information, which will be produced and consumed by the government and citizens (note that both will be providers and consumers, as the interactions can be bidirectional). To understand the nature and characteristics of information is crucial for the design and implementation of e-government systems; and is necessary for effective use of information both in provision of the service and response to it. These services are different from in the traditional form of governance, but supposedly should be equivalent socially and legally. To deliver and enjoy the information-based service through e-government will require an integrated social, legal and technical system that encompasses the technical infrastructure, government and citizens. This system should be built on a sound technical and non-technical basis, covering all semiotic aspects.

References

BCS. (2003, March). Bulletin interview with Andrew Pinder. *The Computer Bulletin*, 16-17.

Chen, H., Zeng, D., Atabakhsh, H., Wyzga, W. & Schroeder, J. (2003). COPLINK: Managing law enforcement data and knowledge. *Comm. of the ACM, 46*(1), 28-34.

De Moor, A. (2002). Language/action meets organisational semiotics. *J. Information Systems Frontier, 4*(3), 257-272.

Gazendam, H.W.M. (2001). Semiotics, virtual organisations, and information systems. In K. Liu, R.J. Clarke, P.B. Andersen & R.K. Stamper (Eds.), *Information, organisation and technology: Studies in organisational semiotics* (pp. 1-48). Boston: Kluwer Academic Publishers.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Gazendam, H.W.M. (2002). Information system metaphors. *Open semiotics resource center: The semiotic frontline, www.semioticon.com*

Hu, M. (2003) *Systems integration and re-engineering using XML/Web Services*. WWW2003, Budapest.

Liu, K. (2000). Semiotics in information systems engineering. *Cambridge University Press.*

Liu, K., Clarke, R., Stamper, R., & Anderson, P. (Eds.). (2001). *Information, organisation and technology: Studies in organisational semiotics.* Boston: Kluwer Academic Publishers.

Liu, K., Sun, L. & Bennett, K. (2002). Co-design of business and IT systems. *J. of Information Systems Frontiers, 4*(3), 251-256.

Marchionini, G., Samet, H., & Brandt, L. (2003). Digital government. *Comm. of the ACM, 46*(1), 25-27.

Medjahed, B., Rezgui, A., Bouguettaya, A., & Ouzzani, M. (2003, January/February). Infrastructure for e-government Web services. *IEEE Internet Computing,* 58-65.

Parsons-Hann, H. (2003). *Information infrastructure for e-policing.* BSc thesis, Computer Science Department, The University of Reading, Reading.

PCIP. (2002). Roadmap for e-government in the developing world. The Work Group on E-Government in the Developing World, Pacific Council on International Policy. Retrieved January 10, 2003, from *http://www.pacificcouncil.org/pdfs/e-gov.paper.f.pdf*

PITO. (2002). *e-Policing strategic framework.* Police Information Technology Organisation, London.

PITO. (2003). *Forward Plan 2003 to 2008.* Police Information Technology Organisation, London.

SOCITM. (2003a). ICT spending up by 25% as councils make progress on e-government. Socitm's IT trends. December 17, 2003, from *http://www.socitm.gov.uk*

SOCITM. (2003b). Small councils' e-government achievements celebrated. Socitm Insight. Retrieved November 16, 2003, from *http://www.socitm.gov.uk*

Stamper, R.K. (1996). Signs, information, norms and systems. In P. Holmqvist, P.B. Andersen, H. Klein & R. Posner (Eds.), *Signs of work: Semiotics and information processing in organisations.* Walter de Gruyter.

Stamper, R.K., Althaus, K., & Backhouse, J. (1988) MEASUR: Method for Eliciting, Analyzing and Specifying User Requirements. In T.W. Olle, A.A. Verrijn-Stuart & L. Bhabuts (Eds.), *Computerized assistance during the information systems life cycle.* North-Holland: Elsevier Science.

Xie, Z., Liu, K., & Emmitt, D. (2003). Improving business modelling with organisational semiotics. In H. Gazendam, R. Jorna & R. Cijsouw (Eds.), Dynamics and changes in organisations – Studies in organisational semiotics (pp. 89-102). Dordrecht: Kluwer Academic Publishers.

Copyright © 2005, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.