iti Techmedia

June 2007

MARKET INTELLIGENCE REPORT

HOMELAND SECURITY

An initial study of the market for Homeland Security, defined as: “private sector products and services which make a substantial contribution to protecting a nation (population, infrastructure and critical assets) against security threats arising from sources other than war”.

EXECUTIVE SUMMARY

This document provides market intelligence into the sector defined as Homeland Security by the Intermediary Technology Institute (ITI) in Techmedia. As awareness of the threats posed by terrorism, criminal activity and natural disasters has increased, the understanding of the potential targets and vulnerabilities of a nation's security has also developed. This has greatly increased the potential scope for the development and deployment of security systems. However the cost of deployment of systems covering (for example) all of a nations entry and exit points against even the most common threats is prohibitive, leading to a focus on the development of practical, real-world security solutions which meet the most critical security needs without excessive cost or impact on existing operations.

For the purposes of this study, and taking account of the focus of ITI Techmedia, the definition of Homeland Security market is:

"private sector products and services which make a substantial contribution to protecting a nation (population, infrastructure and critical assets) against security threats arising from sources other than war"

The report provides an overview of the Homeland Security market, sets out key trends, drivers and inhibitors, reviews the outlook for market development and describes eleven opportunities in the market along with the specific needs identified for each opportunity.

Homeland Security market segmentation is based around identified areas of risk which are realistic targets for government investment

The Homeland Security market is broad and can be segmented in several different ways, for example by threat domain, by government-defined procurement/funding area, by technology or by function. In general these definitions overlap, for example specific detection technologies are deployed in a range of threat domains. In view of this, a pragmatic market segmentation has been adopted (for the purposes of this Report) based around significant areas of risk where there are important unmet needs, not fully addressed by current solutions, and are therefore realistic targets for government investment (in terms of mitigating threats to the nation). This covers the following broad segments:

- Airports
- Land borders
- Seaports
- Infrastructure protection
- Emergency response
- Information security.

Within these segments the Homeland Security market ecosystem is broadly similar:- in that national system contracts are let by governments, typically via a competitive tender procurement process, and targeted by the major, international security system suppliers. Smaller companies specialising in specific security technologies enter the market either in partnership with, or as suppliers to, larger suppliers however in many cases they are subsequently acquired by the larger players. R&D activity in Homeland Security is substantial, comprising significant levels of commercial and academic research.

Homeland security needs vary by region, in part due to geographic differences but also due to relative government spend levels on security. Thus whilst the US is typically the largest potential market for Homeland Security solutions, the UK is the leading European market in several areas (for example CCTV) due to relatively high levels of government spend.

It is also clear that the market has matured following pressure to deploy systems quickly to plug security gaps in the aftermath of 9/11. Thus, a more developed view of the characteristics of successful solutions has evolved:

- Systems must be “real-world”, cost-effective and practical (i.e. with low false alarm rates and low maintenance requirements)
- The needs of end users are increasingly being recognised, favouring solutions with little disruption to standard working procedures and limited additional training requirements.
- Vendors need to offer deployable Homeland Security systems, rather than components which address just one aspect of the problem.

Homeland security markets exhibit a number of key trends

Homeland Security markets have undergone substantial development and growth since 9/11, driven by the actual and perceived threat from terrorist attack and the potential impact on the population, economy and political environment of a nation. Governments have allocated large budgets to these markets because of the need to protect the nation and the political imperative of being seen to be taking the actions required to prevent such attacks.

This high level of threat and threat perception is likely to continue, in conjunction with the following key trends:

- It is beyond the means of even the wealthiest governments to fund protection of the homeland against all threats. Thus some areas of national risk will not be addressed by Homeland Security projects despite the potentially huge impact of an incident
- There will have to be increasing dependence on technology-based solutions, given the vast scale, complexity and diversity of the threats to national security
- Technologies with multiple-uses across Homeland Security, civilian and military markets will be increasingly deployed. This will allow more cost-effective solutions, often led by the development of civil applications.

Significant growth is expected in the Homeland Security sector

Current levels of threat indicate that a substantial Homeland Security market will continue to develop in the short to medium term. Growth is likely to continue, and could increase substantially if further major terrorist incidents occur in the next few years. ITI Techmedia estimates that the overall Homeland Security market will grow from around USD 30 billion in 2006 to USD 90 billion by 2016, a CAGR of 12%, in a baseline scenario which is consistent with current trends. Increased threat levels could see this rise to around USD 190 billion in 2016, as shown in Figure 1.

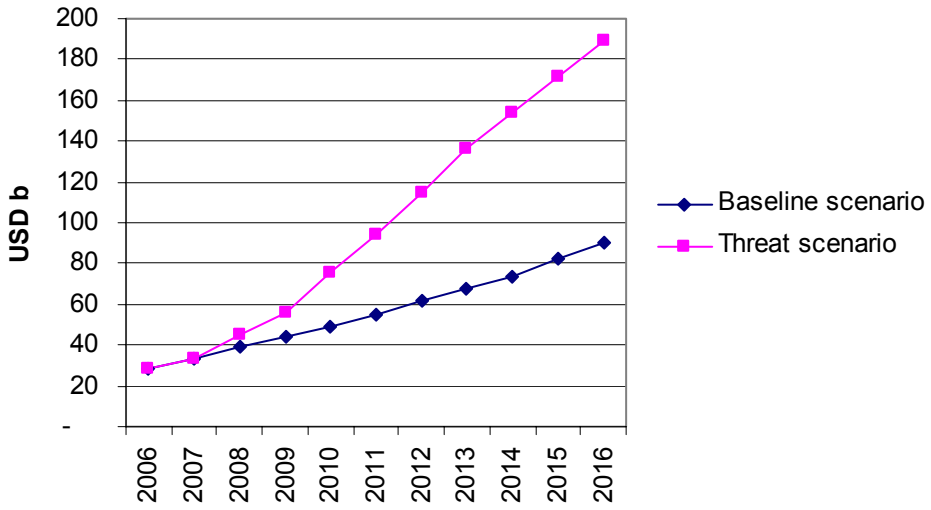


Figure 1: Homeland security market forecast (2006-2016) [Source: ITI Techmedia, Initial data taken from HSRC report “Homeland security and homeland defence outlook 2006-2015]

Opportunities exist in critical threat domains

Within the overall market growth, it is likely that government focus will be directed towards threat domains where critical security vulnerabilities exist. Developing solutions which tackle these vulnerabilities and work in a real world environment will therefore address a substantial market opportunity. Based on a programme of primary research carried out with participants in Homeland Security markets (including system and component suppliers, Government advisory bodies and research groups), the following specific opportunity areas have been identified:

Airport perimeter security – Security systems to protect airport perimeters

Biometrics: Face recognition – Authentication of individuals and other security applications from imaging data, specifically a system which is effective in "walk-by" situations

Border monitoring and control – Sensor, surveillance and intelligence systems for border monitoring integrated with threat analysis methods and intelligence data sources to provide effective support systems for border patrol agents

CCTV – Intelligent CCTV systems integrated with sensor and surveillance systems, embedding effective analytics and intelligence applications within camera and storage control systems

Data analysis and threat detection via intelligent data mining – Identification of threats via the intelligent analysis of huge amounts of data from a range of different sources (including personal data) to determine correlations and patterns which are likely to be important for Homeland Security investigations

Effective threat detection based on data fusion and domain-specific threat modelling and analysis – Threat detection based on the integration and analysis of data from a range of security sensor networks, and domain-specific threat modelling and analysis to enable the discrimination of genuine threat indicators from behaviours which are benign

Explosives detection – Detection systems for explosives at airports, border crossings and critical infrastructure sites, including the integration of data from explosives sensors into an intelligent threat analysis network

Freight container security, monitoring and tracking – Monitoring and tracking of freight containers at seaports and border transit points via a system which is generally affordable by the shipping industry

Information intelligence, privacy and security controls – The proactive gathering, analysis and dissemination of information on potential security threats within a framework which retains the security and privacy of the underpinning data

Video analytics – Recognition of individuals and objects from video data, including both commercial and public sector security applications

Vulnerability assessment – A cost effective visualisation and analysis tool for applications in risk assessment and vulnerability analysis for protection of critical infrastructure.

Using knowledge acquired from the primary and secondary research carried out in the preparation of this report, together with an analysis of which of these opportunities presents the most promising area(s) for ITI Techmedia to investigate further, four areas have been prioritised by ITI Techmedia for further study and engagement with the Membership. These are

- CCTV and video analytics
- Explosives detection
- Border monitoring
- Effective threat detection.

1 INTRODUCTION

1.1 Document Purpose

The purpose of this document is to provide a 'snapshot' view of the Homeland Security sector in order that the ITI Membership:

- has visibility of the market analysis activities undertaken in this sector by ITI Techmedia;
- can gain access to market information relevant to the sector;
- is provided with some opportunities that ITI Techmedia will explore further to identify if they offer opportunities for technology innovation that may form the basis of ITI Techmedia research and development programmes in this area.

This document should not be considered as providing a comprehensive analysis of the competitive environment within the Homeland Security sector. Such an analysis is beyond the scope of this document. This report aims to provide an understanding of Homeland Security and its applications. It also aims to give those who wish to act as players in this space an appreciation of the ecosystem and potential scale of this market.

1.2 Structure and Content

This document provides market intelligence into the sector defined by ITI Techmedia as Homeland Security (see Section 2.1 for the definition of Homeland Security). The information captured within the document has been obtained following the principles of market intelligence gathering (otherwise known as foresighting) established by ITI Techmedia.

During the process of developing this market intelligence report, both primary and secondary market data were acquired and collated. Primary data was collected using interviews with market experts (both public and private sector) and two half-day workshops held with leading companies active in the sector, along with representation from the public sector concerned with national security. The primary data gathering process was augmented by desk research which was used to obtain secondary data from internationally recognised market analysts. Where possible, the source of any data used in this report has been identified. This work was carried out using the services of Sagentia.

- **Section 1: Introduction.** This Section covers the background, aims and scope of ITI Scotland. It also provides a high level description of the 'Techmedia' areas of focus. Further background information can be obtained on the website www.ititechmedia.com.
- **Section 2: Market Overview.** This Section provides a working definition of the Homeland Security market, highlights the main characteristics of the sector, the segmentation of the market and its ecosystem. The main trends, drivers and barriers are identified, and a view of the scale and future evolution of the Homeland Security market is provided.
- **Section 3: Market Opportunity Assessment.** This Section provides an analysis of the top market opportunities identified during the foresighting process. For each opportunity it includes a discussion of the market structure, scale and key players, a vision for the future of the opportunity, together with the expected technology requirements that will meet the market's needs.
- **Section 4: Conclusions and Next Steps.** This Section provides the key conclusions of the report together with a summary of the next steps that ITI Techmedia intends to take in the area of Homeland Security**.**

1.3 Background: ITI Scotland

1.3.1 Economic Context

A global driver for economic growth is the development and exploitation of technology both for present needs and future requirements. Successful economies are underpinned by a vibrant research base which extends from basic science through to pre-competitive research and development, with a clear focus driven by global market opportunities. Scotland has a reputation for world class research in many fields and already undertakes significant research activity in several areas which have the potential to be strong future market opportunities. In addition to the research base, most developed economies have institutes or organisations that promote knowledge generation and increase commercial exploitation capacity. The establishment of such organisations has had significant economic impact over the long term.

1.3.2 ITI Scotland

ITI Scotland is a commercial organisation focused on driving sustainable economic growth in Scotland, through ownership of commercially targeted R&D programmes that deliver world-class intellectual assets.

Specialists from ITI Scotland's three divisions - ITI Techmedia, ITI Energy and ITI Life Sciences - identify technologies required to address future global market opportunities, then fund and manage R&D Programmes and the subsequent commercial exploitation of new intellectual property (IP). This publicly funded company has an active Membership programme for interested parties from the business, research, academic and public sectors. Members enjoy exclusive access to market foresighting (such as that contained within this Report), the opportunity to participate in leading-edge technology R&D Programmes and networking opportunities brought about by regular meetings of a growing network of like-minded organisations.

The ITIs also interact with each other to identify potential overlap or "white space" market opportunities between ITI Techmedia, ITI Life Sciences and ITI Energy.

The ITIs are a centre or "hub" for:

- identifying, commissioning and diffusing pre-competitive research that is driven by an analysis of emerging markets
- managing intellectual assets to maximise commercial and economic value.

An active Membership is core to the ITI Scotland model. It is open for Membership to companies and research institutions willing to actively participate in its activities. ITI strategy and operations are actively guided and supported by Members. ITI Scotland seeks Members with a broad global perspective on markets and new technology directions, as well as a local focus, to ensure that propositions will be transferred effectively into the Scottish economy.

1.4 Definition of the Techmedia Sector

ITI Techmedia is centred on the development and creation of commercial opportunities encompassing the communications technologies and digital media sectors. The activities of the ITI will bring Scotland's economy to the cutting edge of emerging markets by allowing local companies to access and build upon pre-competitive technology platforms developed by the ITI.

The term 'Techmedia' arose out of the need to reflect the market evolution of communications technologies and digital media. The overall trend in the marketplace is one governed by a value chain ranging from content/application generation through delivery to consumption. Content, service

provision, delivery channels and, enabling and managing technologies can no longer be treated in isolation and ITI Techmedia seeks to operate across the value chain.

The key to identifying opportunities for research and development lies in a process called Market Foresighting which involves detailed market and technology analysis to identify trends, evolving requirements and potential demand for new technology. ITI Techmedia compiles the output of this activity into Market Intelligence Reports which are published to Members. This market foresighting informs our R&D Programme identification process.

The Techmedia sector is potentially very broad. Hence a phased approach to market foresighting has been adopted. Previous foresighting has concentrated upon seven major market areas:

- Health
  - including a further Report on technology opportunities in Remote Health
- Commerce and Finance
- Learning and Education
- Communication Services
- Entertainment and Leisure
- Digital Cinema
- Nanotechnology

To date, these foresighting activities have helped ITI Techmedia to identify seven R&D Programmes:

- ***Games-Based Learning*** - to develop a differentiated creation and authoring platform to simplify the creation of games-based learning content. Completed January 2007.
- ***Machine-Readable Security Tagging*** - to develop an end-to-end system solution, featuring a range of component technologies required to protect brands and combat the growing global threat to products from illegal counterfeit activity. Completed March 2007.
- ***Ultra-wideband Wireless Communications*** - to develop the components, system and network management elements for ultra-wideband wireless technology in consumer markets
- ***Condition-based Monitoring*** – to apply sensors and networks technology to condition-based monitoring for predictive intervention in animal health matters
- ***Biosensors*** - to create a technology platform that will facilitate both diagnosis and treatment of infectious diseases
- ***Online Game Development*** - to establish a world-class development platform to facilitate the efficient production and distribution of online PC, console and hand-held games
- ***Backlighting Using Polymer Optics*** - to develop a novel backlight platform for liquid-crystal flat-panel displays to improve viewing quality, reduce weight and improve power efficiency at lower cost

2 MARKET OVERVIEW

This section presents an overview of the Homeland Security market and an analysis of its evolution together with the main drivers that will influence this evolution. As such, this section provides:

- a definition of the Homeland Security sector
- the high-level market segments within the Homeland Security sector
- a description of the ecosystem, its characteristics and main players within it.
- the main trends, drivers and inhibitors
- a forecast of the evolution of the Homeland Security market

The objective of the foresighting process is to identify areas of opportunity for the development of technology platforms which address unmet market needs that:

- are unlikely to be satisfactorily addressed by current solutions or approaches in the short term
- have the potential to be addressed in the medium term by new, technology-based developments
- are likely to provide a significant revenue opportunity for market participants in the medium term.

The Section provides a framework for the identification of such opportunities in Section 3

2.1 Market Definition

For the purposes of this Report, the Homeland security market is defined as

"private sector products and services which make a substantial contribution to protecting a nation (population, infrastructure and critical assets) against security threats arising from sources other than war"

Specific examples include:

- preventing unwanted individuals, materials and objects from entering a country's borders
- protecting the infrastructure of a country, including utilities, transport systems and critical sites
- dealing with natural disasters and other emergencies
- defending the population against terrorist activities and actions within a country's borders.

Dealing with these threats requires effective Homeland Security applications covering a wide range of areas, ranging from security procedures at key entry and exit points (e.g. airports, seaports, borders), detecting hazardous materials (e.g. nuclear, chemical and biological agents, explosives), and intelligence operations (e.g. surveillance, tracking, detection). These applications require a broad range of enabling Homeland Security technologies to provide the basis for their effective operation. These technologies include, for example: biometrics, identity cards, detection systems, screening systems, CCTV surveillance, unmanned aerial vehicles, RFID tracking and tools to integrate and analyse security data from different sources.

As well as providing the required functional capabilities, deployment of these technologies should provide operational benefits such as cost-effectiveness improvements, drawing together and making better use of existing information, allowing real-time analysis and information provision or improved prediction and detection of threats. Enabling Homeland Security technologies are also likely to have significant commercial application in market sectors outside the Homeland Security domain.

Military markets, for example weapons targeting systems or systems to protect military installations, are excluded from this definition. However there is clearly a degree of overlap between military and Homeland Security systems in terms of technology and functionality in some cases e.g. similar surveillance systems could be deployed around military bases or at land borders. In these cases the focus in this report is on civil applications of the relevant technologies.

Geographically, major Homeland Security markets exist in the US and Europe, within which the UK is the lead adopter in many areas. This report focuses on European market requirements.

2.2 Market Segmentation

As defined above, the Homeland Security market is broad and encompasses a wide range of functional applications and technologies applied across different threat domains. However functional applications are not specific to threat domains, for example explosives detection is relevant for both airport passenger screening, and for scanning trucks passing through land borders. Similarly, relevant technology capabilities may be applied in more than one Homeland Security area; for example secure, interoperable communications links are required to transmit data between ground sensors and monitoring cameras, or to allow first responder personnel from different services to communicate in emergency response situations.

In view of this breadth and complexity which exists within the Homeland Security market, the market may be segmented in several alternative ways (e.g. by threat domain, by procurement/funding area, by technology, by function etc.).

Therefore a pragmatic Homeland Security market segmentation has been adopted, based around identified areas of Homeland Security risk which are realistic targets for government investment (in terms of mitigating threats to the nation). This covers the following broad segments:

Airports	Protection of airports including passenger, luggage and cargo screening, access control and airport perimeter security.
Land borders	Protection of land borders – principally the US southern border and land borders in Eastern Europe and the Middle East. This includes protection of remote border regions and border crossing points, for example using ground sensors, border monitoring and control systems or unmanned aerial vehicles.
Seaports	Protection of seaports and other coastal infrastructure. This includes areas such as freight container security, underwater security, coastal radar and imaging systems etc.
Infrastructure protection	This includes protection of important national infrastructure, for example power generation plants, transit points and drinking water supply.
Emergency response	Response to national emergencies, for example natural events or terrorist attack. This includes areas such as interoperable communications systems, emergency response coordination and vulnerability assessment.
Information security	Overarching physical Homeland Security segment is information security, which includes Homeland Security threat identification and detection, for example through security event correlation, data mining and information intelligence.

Each of these segments includes areas of opportunity within the overall Homeland Security market. These areas combine significant security concerns with functional needs which may not be fully addressed by current solutions.

This segmentation is illustrated in Figure 2 below, and highlights the high degree of overlap between different aspects of Homeland Security. For example airports, seaports and borders are all part of a broader "entry point and transportation security" domain, and information security has a vital part to play across many aspects of physical Homeland Security solutions. In addition to information security, emergency response sits across all areas of Homeland Security but in a reactive way rather than a predictive capacity. The remaining segments are more preventative in nature and cover the different locations that an event may be targeted against. The main areas of opportunity in each segment are discussed in the following sections.

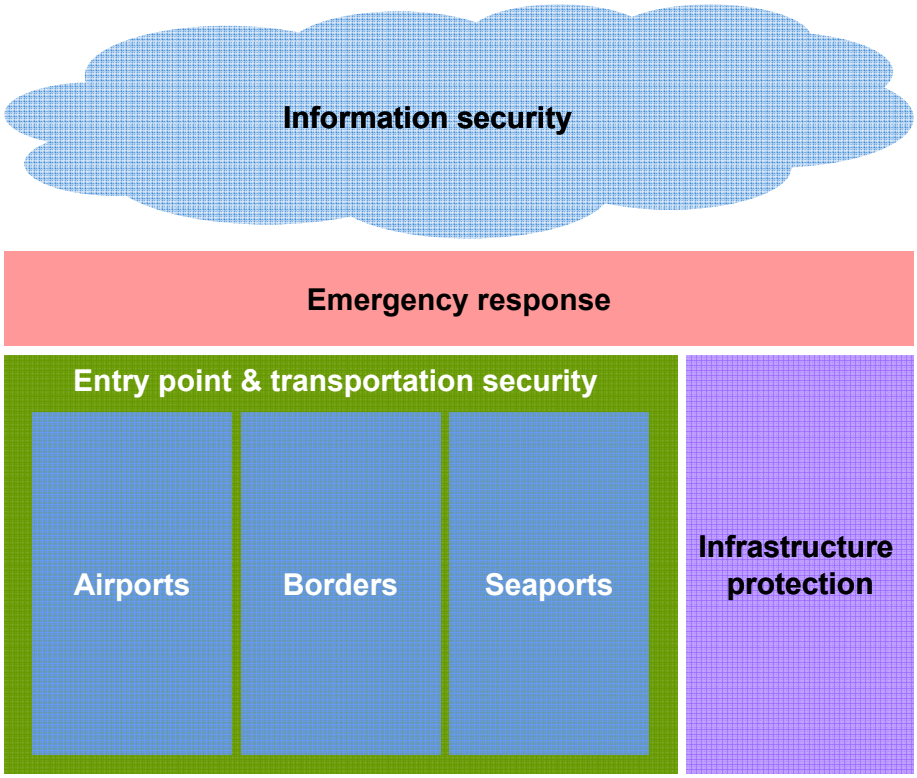


Figure 2: Homeland Security Market Segmentation [Source: ITI Techmedia]

In the following sections, these segments are explored in further detail.

2.2.1 Airport security

Since 9/11 considerable attention has been directed towards security measures at airports. In addition to enhanced screening for potential weapons via X-ray scanners and body searches, additional effort has been focussed on screening passengers for carried explosives, with the introduction for example of handheld explosive detection equipment and "puffers" to detect explosives' vapour. Recently concern has focussed on liquid and paste explosives (or explosive precursors) which can be carried in sealed consumer goods receptacles.

As well as passenger screening, additional measures have been taken to screen checked baggage and air cargo for explosives, for example the installation of checked baggage explosive screening equipment at US airports in 2004. In contrast, less effort has been directed towards systems for detection of chemical and biological agents at airports, largely due to the lack of cost-effective detector systems for these agents.

Whilst security for passenger and cargo routes has been significantly improved, less obvious attention has been directed towards other critical aspects of airport security. Secure access to airports for very large numbers of employees is required, and improved authentication technologies have been deployed to achieve this e.g. iris recognition technology is deployed for 32,000 users (both workers and business travellers) at Schiphol airport.

In addition, surveillance and security control of airport perimeters is coming under increasing scrutiny after cases of unauthorised individuals gaining access. Airport perimeters are extremely long and, in addition to physical security measures, surveillance and command and control systems are increasingly being deployed to secure airport boundaries. This includes the use of CCTV equipment as well as alarms and sensors.

2.2.2 Land border security

Maintaining effective security at important land border crossing points and along lengthy, ill-defined borders in remote locations has proved difficult. The US southern border, Eastern-European borders and land borders in the Middle East are the most important areas in this market. For example in the US considerable efforts have been made to deploy technology-based solutions on parts of the US-Mexican border, but these have been unsuccessful. As well as the sheer scale involved (it has been estimated that 276,000 sensors would be required to cover the entire US southern border), surveillance systems have to cope with adverse weather conditions and lack of support infrastructure (power, communications links). Trial systems have resulted in high false alarm rates, which overwhelm patrol agents' capacity to respond.

In view of these issues, funding has been directed away from technology and more toward traditional, proven solutions – more officers and trained dogs. Innovative approaches to patrolling remote borders have also been tried. For example unmanned aerial vehicles carrying surveillance sensors and communications equipment have been tested in the US, however these have not yet reached an affordable system price in this market and regulatory issues have not been resolved. It is possible that military technology may provide solutions in this market, for example unattended self-networking and self-powered ground sensors may be capable of surveying difficult areas remotely, but this is likely to be a long term vision. Ground penetrating radar has been tried to find drug-smuggling tunnels under the Mexican border, but in practice human intelligence has been much more effective in discovering the location of the tunnels.

Security at border crossing points presents different challenges. Important concerns are screening freight, checking individuals for illegal entry and detecting unauthorised materials. Although technologies exist to perform these tasks, in general the cost of these systems and the constraints they impose on throughput have proved a significant barrier to deployment. For example, scanning a container, trailer or railcar to detect shielded nuclear material is possible using imaging technology, but not without introducing unacceptable delays. Mature, proven biometrics are available to perform authorisation of individuals, but this requires effective enrolment processes and currently requires attended screening with the delays and cost impact this implies.

2.2.3 Seaport security

The majority of goods entering countries via seaports are not screened before entry – for example only 5-6% of containers passing into the US via its ports are screened. This represents a significant security issue, as containers could contain materials useful to terrorists as well as other illegal contents such as drugs or weapons. The principal difficulty preventing the introduction of screening systems is cost – the profit per container generated by the shipping industry is relatively low and is insufficient to bear the cost of introducing effective security systems. Technologies exist to meet this security need, comprising for example RFID identification and tracking, and monitoring of container tampering and condition monitoring en route, however governments have generally not allocated the funding required to address this issue and have preferred to target containers entering the country from specific, high risk ports of origin.

Issues in terms of screening containers at land borders equally apply to ports – for example imaging systems to non-intrusively scan containers passing through ports (for example to detect

shielded nuclear material) are expensive, and the impact on container throughput time is currently too great to be commercially acceptable.

In some cases container security systems are being introduced by goods owners, as a part of their logistics processes. Ensuring security of their supply chain is a key element of this, for example Starbucks is using a security system based on RFID to secure its coffee supplies and protect its brand.

As well as considering the goods passing through seaports, ensuring the security of the ports themselves is a significant concern. For example, the cost of disruption at a major US port has been estimated at ca. USD1 billion per day. Security spending at ports has focussed on physical security measures such as lighting and fencing, which have been the most basic security gaps to fill, rather than on measures involving the use of technology e.g. using sonar or unmanned underwater vehicles to protect against threats from divers with explosives or the use of imaging and radar systems to track unauthorised small boats entering the port. In general such systems have only been implemented on a trial basis, and there has been little movement by governments to fund solutions in this area. This situation could change, for example if a major terrorist attack occurred via this route.

2.2.4 Infrastructure protection

Infrastructure protection encompasses security applications at a wide range of government and commercial sites, including for example power stations, oil and gas terminals, water supply access points, dams, and communications centres. Currently Homeland Security measures involve monitoring and surveillance systems as well as access control measures to restrict access to authorised personnel. Vulnerabilities in these infrastructure sites are being analysed by governments, but from a market perspective often there is a lack of a “kick-start” incident to trigger significant government spending. For example drinking water systems are largely secured by simple, low-tech approaches rather than by real-time toxicity detection systems, however this could change if a high-profile incident occurred.

In this context advanced (IP-based) CCTV systems are growing in importance. Based on the recognition that human monitoring of increasing amounts of CCTV data is becoming impractical, efforts are being made to automate the scanning of camera data and translate these into real-time alerts which have a low false alarm rate. This is a difficult challenge, as it requires significant breakthroughs in (for example) effective, automated behaviour analysis or in the development of intelligent threat analysis based on inputs from other security sensors alongside CCTV data.

A critical capability in this area is video analytics, which could provide a broad range of functions including the ability to authenticate individuals from CCTV data, recognise objects and analyse scenes. This in turn enables higher order meta-data to be created which supports the automated scanning of CCTV camera data. Again, this is technically difficult.

A range of existing, relatively mature biometric technologies can also be deployed for access control at key infrastructure sites, for example iris recognition and fingerprint reading. For these technologies, significant anti-spoof measures are required for unattended secure operation, rendering them expensive. Similarly whilst face recognition technology has the benefits of being non-contact and non-invasive, it requires high resolution image capture which is currently expensive for access control applications.

The implementation of national ID cards would provide a ubiquitous identity mechanism; however this is limited by the level of adoption/implementation, which is itself limited by political acceptance. Achieving a critical mass of holders who would accept the routine use of the process could result in a range of opportunities, including access control and commercial applications.

2.2.5 Emergency response

Response to natural disasters and other emergencies falls within the homeland (or national) security domain. Particularly relevant are areas where significant operational difficulties have occurred during the response to emergencies such as 9/11 and hurricane Katrina. Such events require co-ordination and interoperable communications between emergency response teams.

A key requirement is that first responders to major emergencies from different “blue light” services are able to communicate with each other. This requirement has significant implications in terms of procurement of wireless communications systems which are able to interoperate, provision of sufficient radio spectrum with the right propagation characteristics to provide sufficient capacity for emergency services (for example mobile networks are typically overloaded quickly following major incidents). Advanced communications systems may be needed, for example using elevated antennas which can work in a high-rise building environment, systems which provide location information for response team personnel within areas, buildings and structures and rapidly deployable, self-managing networks which can be set up rapidly in emergency situations.

In addition to establishing communications networks, command and control systems are needed to co-ordinate emergency response across (for example) central control, front-line staff, field data and medical facilities. This is likely to include security and communications software – middleware – which enables secure access control and information flow between response teams.

It is also likely that vulnerability assessment will increase in importance, driven by the need to target security budgets appropriately and according to ongoing threat assessment and risk analysis. This may require improved methods for carrying out vulnerability assessment, and visualisation tools to integrate understanding and classification of threats with mitigation options and security strategy.

2.2.6 Information security

Developments in information security are influencing wider areas of Homeland Security. Information security is defined here as the broader use of information and data to meet Homeland Security objectives rather than simply maintaining the security of the information itself. Recognising that no government can provide sufficient funding to plug every security gap, significant emphasis is being placed on collecting and analysing data from a wide variety of government and non-government sources to identify threats and deal with them before an incident occurs. Such deep data mining to identify patterns and correlations indicative of security concerns has challenging performance requirements and high “tuning” costs. Substantial privacy concerns must be overcome, but it is likely that significant developments will occur in this area. This is evidenced by the development of “fusion centres” in the US, to address a wide range of threats including terrorism, international gangs and smuggling.

A further important area of development is in systems for detecting and preventing intrusions into physical or data networks based on intelligent systems which are capable of distinguishing indicators of genuine threats from behaviours and sensor data which are benign. Such systems operate at a level of synthesised intelligence based on analysis of larger aggregated data-sets, and are likely to form a key component of many Homeland Security systems in the medium term based on effective discrimination of genuine threat indicators. This is consistent with a growing trend towards sensor fusion – integrating (and subsequently analysing) data from a range of different security sensor inputs, for example correlating data from seismic sensors with appropriate imaging data to assess whether an event is real or is a false alarm e.g. an animal intrusion.

Many areas of information security are subject to significant uncertainty due to the differing levels of importance placed by different governments on privacy concerns. This is likely to give rise to opportunities for systems which ensure the protection of personal information e.g. by

ensuring that data which is analysed for security correlations cannot be identified unless a positive threat is identified.

2.3 Characterisation of the Ecosystem

The Homeland Security market and underlying ecosystem is discussed below covering:

- the general characteristics of the Homeland Security market
- the ecosystem and types of players within the market
- the characteristics of a successful solution
- the geographical variation in the Homeland Security market

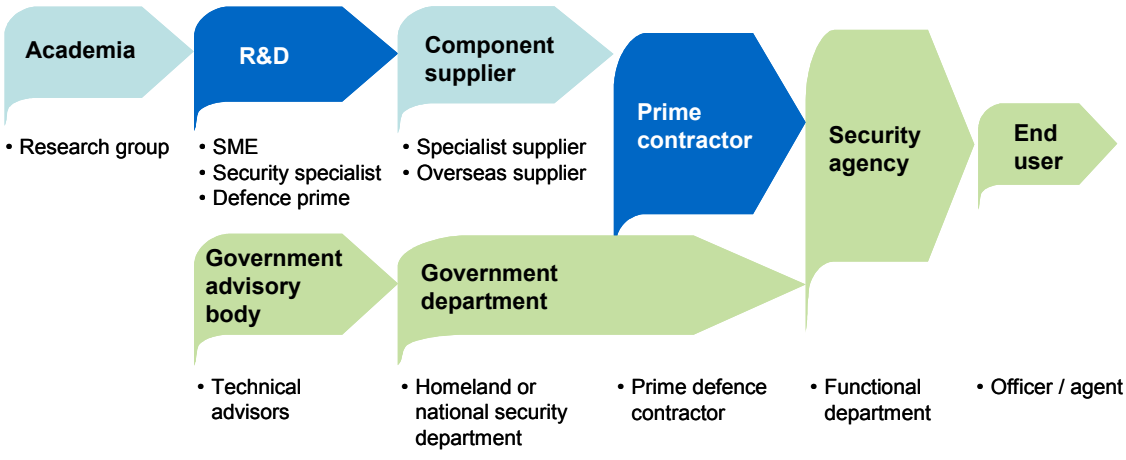
2.3.1 General characteristics of the Homeland Security market

The Homeland Security market is defined by national governments, in that it is governments that largely spend on Homeland Security projects that impact on national security. This fundamental fact has major implications – spending priorities and decisions are often reactive, and can be driven by emotion and short term political factors (to demonstrate action) rather than by a rational analysis of threats. Thus government spending is unpredictable and hence funding and project timing in Homeland Security segments are unclear. In some senses Homeland Security is a "fashion" market, in that end user wants are distorted by the process of setting spending priorities.

Thus, some areas of national risk have not been addressed by Homeland Security projects despite the potentially huge impact of an incident. For example, there is no coastal security system in the US to prevent entry of people or materials which could contribute to a significant terrorist attack. Indeed, in all likelihood it is probably beyond the means of all governments (including the US) to fund national programmes to protect the homeland against all foreseeable threats. Hence some areas of market need are likely to remain unfunded.

2.3.2 Homeland security market ecosystem

National Homeland Security programmes are significant contracts and attract major players, ranging from large defence contractors such as Lockheed Martin and Northrop Grumman in the US, Thales and Selex in Europe, to the larger systems integrators bidding for the more IT-related systems. Smaller, technology-based companies participate either through carrying out funded R&D and forming partnerships with major players. In many cases these small companies are acquired by larger companies seeking to broaden their Homeland Security portfolio. This market ecosystem and value chain (broadly: governments, prime contractors, smaller specialists) is shown in Figure 3[1] and discussed in more detail below.



[1] Green = public sector, Blue = private sector & research

Type	*Definition*	*Examples*
Academia	Academic research group working on security technologies	Security Engineering research group, University of Cambridge
R&D group	R&D (carried out by SME, independent research group or large defence contractor)	TRL Technology (secure radio communications)
Government advisory body	Public sector technical advisory group	Home Office Scientific Development Branch (HOSDB)
Component supplier	SME supplying component technologies, typically in partnership with a prime contractor	ObjectVideo (intelligent video on a chip market leader)
Government department	Government body with responsibility for letting Homeland Security contracts	Home Office (UK)
Prime contractor	Large security or defence system supplier, typically responsible for delivering a security programme	Thales, GE Communications
Security agency	Functional public sector group responsible for specific security functions	U.S. Coast Guard
End user	Field agents of a security agency	Border patrol agent (U.S. southern border)

Figure 3 Homeland Security generic value chain [Source: ITI Techmedia]

The general characteristics of the Homeland Security ecosystem and the players who operate in this market are discussed below:

Government procurement is typically via competitive tender

As already noted funding decisions can be influenced by political considerations as well as logical analysis. Thus, solutions which seem to be a path of high political risk (e.g. aggressive use of biometrics in Europe) may find no real market.

In addition, many procurement processes are based on issuing a requirement specification against which vendors tender. Since requirements depend on what can actually be achieved by vendors, difficulties can result. Examples include commissioning systems which don't meet specification performance targets, or don't work in the real world. In general, governments lack the resources to validate vendor claims.

Large contractors target national system contracts

Many major vendors have moved into Homeland Security markets by a combination of repurposing their military solutions, developing new products to fill gaps and acquiring other companies to cover more of the market. Such vendors are then positioned to bid for national contracts. Clearly this is high risk – some vendors have announced withdrawal from the market in response to lack of contract success. Timing is also an issue, in terms of building capability to win a bid process which may be delayed or withdrawn. In some cases, Homeland Security teams have been reduced to dormant status, ready to be activated in response to a pick-up of activity in the market.

Smaller companies

Smaller companies addressing Homeland Security markets tend to

specialise in specific Homeland Security segments

focus on specific segments within the overall market. Homeland security is typically addressed alongside other, private sector markets, in order to reduce the risk of being unsuccessful in Homeland Security contract bids. Smaller companies may find it difficult (at least initially) to obtain the level of trust required to gain insights into specific unmet needs from government organisations. In addition, they may have problems acquiring security clearance for foreign markets (although setting up an appropriate overseas company and recruiting suitably qualified nationals are ways around this problem). As already noted, achieving a technology leadership position in key Homeland Security areas is likely to lead to acquisition attempts by larger players.

R&D activity in Homeland Security is substantial

Given their background in military markets, it is no surprise that the major Homeland Security vendors such as Thales, Qinetiq and GE Security have substantial R&D resources they can bring to bear. In addition, smaller specialists have strong technical capability, and there are often several companies competing within a Homeland Security market segment, often with different technical approaches.

Academic research also plays an important role – several Homeland Security areas require fundamental advances to provide the possibility for feasible solutions to emerge.

The ecosystem is broadly similar across market segments

As most Homeland Security markets are defined by government spending, in broad terms the procurement process is similar across different Homeland Security segments and the characteristics of the ecosystem will be the same. However the specifics will differ, in terms of the department responsible, the likely bidders, partnership dynamics, timescales and funding routes etc.

Homeland security needs vary by region

The inherent (i.e. based on threat analysis) requirements for Homeland Security solutions vary depending on the geography and political situation of the region concerned. Thus, the US is different to Europe, and traditional defence markets like the Middle East are different again. This is discussed in more detail below.

2.3.3 Characteristics of successful solutions

The Homeland Security market has matured following its origins in the aftermath of 9/11. This is largely based on experience in the US of spending large budgets on technology-based solutions which have often failed to meet the operational needs of end users, and have not resulted in the envisaged security benefits. This experience is being recognised in government procurement practice, and hence has a direct impact on suppliers. Important implications of this are discussed below.

Awareness of specific needs may be difficult for new entrants into Homeland Security markets

Whilst the broad needs being addressed in Homeland Security markets are in general openly defined, specific unmet needs are typically not made explicit by governments to avoid advertising vulnerability and to keep attackers unaware of the extent of capabilities in respect of a specific counter measure. The absence of any clear indication of gaps may increase deterrence and caution on the part of attackers to a greater extent than if all shortcomings are well known. Awareness within industry of the current and future needs may only be available to major, trusted suppliers.

The lack of clarity of unmet needs is an important characteristic of this market. There is a subset of capabilities, the existence of which are secret – meaning that some needs that are implied by gap analysis of current technologies may not exist in practice. Likewise there are some real needs and gaps, for which there is no explicit acknowledgement in the public domain.

The needs of end users are increasingly being recognised

In many Homeland Security markets, solutions have been too technology-focussed and have failed to provide a system that is robust and operationally useable – for example high false alarm rates of border control sensors have lead to the alarms being ignored. In many cases, the unmet need is often in achieving a usable system, rather than better technology. Thus some commentators have suggested that a better use of money would be to increase the availability of appropriately trained personnel or to provide engagement, discussion and training to people on the ground.

In many cases Homeland Security systems are technically feasible, but have too high an impact in terms of the changes to working practices that they would require. For example implementing cargo scanning systems requires interworking between trucking, port operating and scanning companies. In practice this is a significant barrier as changes in attitude by end users who will be given the tasks of operating the new solutions are needed.

Systems must be cost-effective and practical, and must be "used every day"

Clearly, Homeland Security systems must be affordable by users. This means implementation of the whole system, i.e. including training, process change, impact on other processes etc. Critically systems must not generate adverse effects – false alarms, additional bottlenecks etc. – otherwise they will simply not be used. Some users are also questioning the value of investing in and supporting systems which are only of use in exceptional circumstances; as one department put it: "if we don't use it every day, I don't want it".

Many Homeland Security technology components are mature

Many of the underpinning Homeland Security technologies are now mature in technology development terms, e.g. fingerprint recognition, iris detection etc. The key issue is how these technologies are used in systems and processes that will work in the real world. This is partly a traditional systems engineering task, e.g. making user interfaces work, handling errors and exceptions, and designing the kiosks, gates etc. so that the technology works in the application environment.

Vendors need to offer Homeland Security systems rather than components

For many Homeland Security applications, the cost of the technology element (cameras, sensors etc.) is a small element of the overall system cost. Increasingly, attention (and hence funding) is directed to aspects such as training, system integration, procedure development etc. Systems must be engineered to be useable in the real world, and vendors must supply complete systems not components.

2.3.4 Geographic variations in the Homeland Security market

Given that Homeland Security market spend is largely defined by governments in response to events which have occurred and to perceived threats faced, Homeland Security markets vary by country. The main regional differences are outlined below.

The US

The US has invested massively in all major areas of Homeland Security, through the Department of Homeland Security which plans to spend USD30.9 billion in 2007. Much of this funding goes to heavyweight defence companies re-purposing military solutions, who have the resources to undertake the extensive lobbying required. Accessing this funding is very hard, and it is very tough to compete with the large US defence companies. There are not many customers, and their decisions are not predictable.

Since 9/11 US government funded programmes have covered virtually all Homeland Security areas, however it is increasingly recognised that there is not enough money to plug every gap and that much of the spending has resulted in slow and ineffective project rollout and slipping schedules. There is growing concern about lack of results from technology-based solutions.

R&D spend is directed through the Homeland Security Advanced Research Project Agency (HSARPA), which covers funded Homeland Security R&D accessible to small (US) businesses. Whilst the 2007 Homeland Security science and technology budget is USD1 billion, participants face a rigorous assessment process. Market entry (for companies with new technology-based solutions) is very difficult for non-US companies – the US procures from companies they have funded, and there is already a shortlist in place. Recently concern has been expressed about intellectual property risks – national security is the overriding consideration and there has been speculation that IP owners may lose “technology ownership” cases in the US.

Europe

European spending on Homeland Security is far lower than US expenditure, and varies by country but to a limited extent. At a high level, the Homeland Security needs of European countries are broadly similar, and it is possible to have a common overview of the potential “European” market across common threat domains such as borders (screening), airports (biometrics) and seaports (container ID and screening). What differ are specific, micro level factors for each country, for example there are many different potential buyers (e.g. government agencies/public sector authorities) and these are different for each country. As in the US major European defence companies re-purposing military solutions are addressing the Homeland Security needs of major European countries. There is strong emphasis on setting pan-European standards, e.g. for border control and wireless communications.

Pockets of high demand exist in particular countries – for example the UK is the lead market in CCTV, whereas other countries may have lower levels of demand. Specific events also have a major impact, for example the London Olympics in 2012 will have a significant impact on the UK resilience (Homeland Security) market.

Other markets

Although smaller than the US and Europe, other significant Homeland Security markets exist:

- In general the Far East does not have the political risk caused by the civil liberty concerns present in the west, and hence Asian countries may well be early adopters of Homeland Security technologies
- Countries in the Middle East are focussed primarily on land border security, and there is particular interest in border protection.

2.4 Market Trends, Drivers and Inhibitors

A number of drivers and trends will affect the development of the Homeland Security market.

> **A trend is a discernible pattern of change, which can be linear, accelerating or decelerating. An example of a trend is: the increasing average age of the UK population.**
>
> **A driver is a factor that directly influences or causes a change in a specific market. An example of a driver based on the above trend is: the need for easier to use interfaces in mobile phones making them accessible to the ageing population**

The overall major trends and drivers impacting on the Homeland Security sector are discussed below.

Key drivers

- Since 9/11 the key driver for investment in Homeland Security Technologies is the potential and perceived threat of a terrorist attack to national security, together with the related impact on the economic and political environment. This is likely to continue.
- Governments have the public support to allocate large budgets to these markets because of the high publicity and related public fear from any terrorist event. There is an obvious political driver to be seen to be doing all that is possible to prevent such attacks
- Private sector becoming increasingly aware that they need to ensure business survival if faced with a disaster scenario
- In Europe the land borders and level of migration of people increases the opportunity and vulnerability to attack

Key trends

- Increasing dependence on technology solutions given the vast scale and diversity of the threats to national security
- Beyond the means of governments to fund protection of the homeland against all threats. Areas of national risk not addressed by HS projects despite the likely huge impact of an incident
- Multiple use technologies used within Homeland Security, civilian and military contexts allows more cost-effective solutions

There are some specific inhibitors to the Homeland Security market namely:

- It is highly dependent on government spending and hence a country's financial position. In the US the federal deficit is around USD8.8 trillion[2] and growing which may cause a reduction in budgets for Homeland Security programmes.
- There are inherent problems in measuring success of programmes that are preventative in nature. It is impossible to gauge if deployment of an effective measure has prevented an event from ever being planned.
- It is difficult to maintain momentum of spending if no further major attacks occur

In addition to these generic Homeland Security drivers, there are threat specific drivers such as:

- Airport Perimeter Security Market:
  - The significant growth in air travel has led to new or expanding airports. This is particularly true in South America and Asia. These new buildings require security solutions thus driving growth in the market.
- Video analytics market:

[2] Source: http://www.federalbudget.com/

- Due to the huge number of video cameras that have been deployed for security purposes there is a significant drive and opportunity to increase the integration of the data from these surveillance systems. This creates a huge opportunity for video analytics.

These are discussed in detail for each of the key market opportunities in Section 3.2.

2.5 Homeland Security Market Outlook

Public sector Homeland Security markets are risky to address, in the sense that even if end users want a specific, available solution which meets their exact needs, a budget from government might not be forthcoming. In addition, funding may be driven by the need to respond to individual incidents, which may not in the future be the most important areas to defend against. Measuring the effectiveness of Homeland Security programmes is difficult – it is hard to assess the "incidents that have not happened" as a result of counter measures already put in place.

Much of this may be explained by the psychology of the response to Homeland Security threats such as terrorism – although much greater causes of death, such as road traffic accidents, receive only a small proportion of the Homeland Security market spend, the nature of the Homeland Security threat is perceived as within the sphere of control of coordinated government response and therefore governments need to be seen to take action. This situation may change, for example if the threat of global terrorism recedes, or if the perceived risk to nations from natural disasters (e.g. hurricanes in the US) rises. Alternatively, the Homeland Security market might expand, if for example future terrorist aggressions occur which are orders of magnitude worse than current experience, or if the mitigation of threat through Homeland Security (as opposed to overseas military engagement) becomes accepted as being less prone to incite the grievance causes of terrorism and represents a more effective use of capital.

In order to deal with this wide range of possible scenarios, many companies addressing the Homeland Security market are doing so in parallel with other activities. Thus, R&D focuses on developments with application in both Homeland Security and private sector markets.

In the forecasts laid out in the rest of this section two scenarios are considered:

- Base line scenario: the level of perceived threat is assumed to continue as it is today. There are no major incidents in the period considered however there is continued terrorist activity with the implication that the threat of a major incident still exists

- Attack scenario: it is assumed that a major terrorist incident occurs during 2008 at a similar scale and impact as 9/11. This significantly increases the perceived threat of further attacks and correspondingly, government spend on Homeland security grows

Figure 4 outlines the worldwide Homeland Security market in these two scenarios. It should be noted that this estimate aims to portray the actual spend which may be smaller than government allocated budgets (outlay). This is viewed to be a more accurate representation of the addressable market for Homeland Security providers and excludes money that is perhaps allocated but never spent (i.e. no technology available to meet the market need or lack of administrative resources to ensure budget spend in allocated timeframe). The forecasts do not include expenditure associated with government funding of police activities associated with terrorist activity (such as identification and prosecution of criminal activities).The Homeland Security market includes all business activities (technologies, other goods, services and generic elements which are common to other industries but used within a Homeland Security environment, such as computers and uniforms).

It is estimated in the baseline scenario that the overall Homeland Security market will grow from around USD30b in 2006 to USD 90b by 2016. This represents a CAGR of 12% which is a conservative estimate compared to a CAGR of 14% observed on the worldwide Homeland Security outlay from 2003-2006.

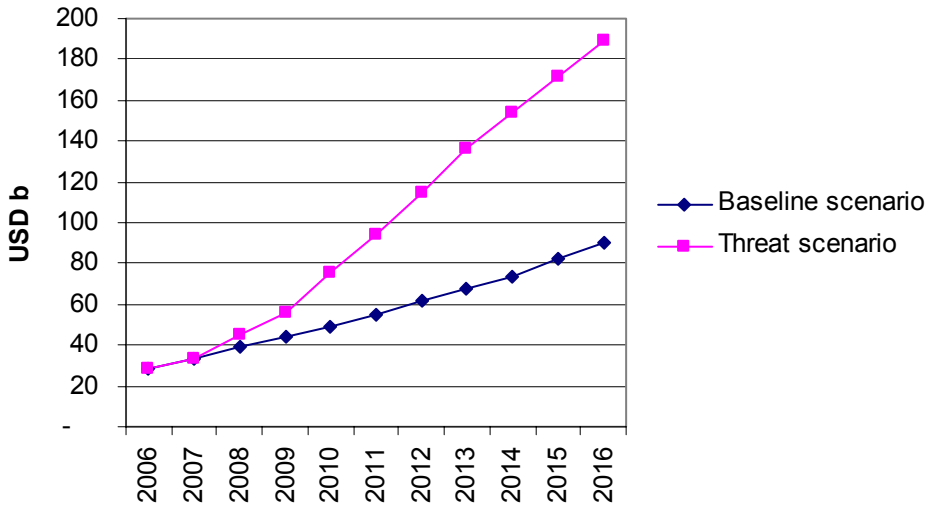


Figure 4: Homeland security market forecast (2006-2016) [Source: ITI Techmedia, Initial data taken from HSRC report "Homeland security and homeland defence outlook 2006-2015]

During the remainder of this section the geographical and application segmentation is considered on the baseline scenario. Obviously within the threat scenario the focus of additional spending will depend on the form and geographical target of the particular major terrorist incident.

2.5.1 Geographical Homeland Security forecast

As discussed the relative scale and focus of Homeland Security market spend varies country by country. Figure 5 illustrates the relative scale of the Homeland Security market by geographical region. It is clear that it is heavily dominated by the US comprising 55% of total market in 2006 falling to 43% by 2016. The EU is the second biggest and growing market with 23% share in 2006 growing to 30% by 2016.

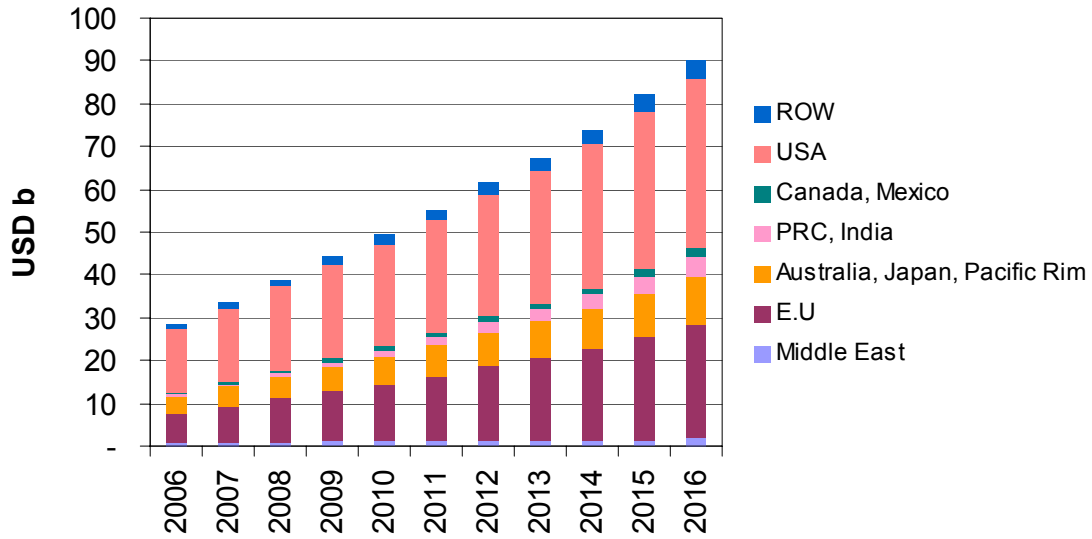


Figure 5: Homeland security market forecast (2006-2016) by geography [Source: ITI Techmedia, Initial data taken from HSRC report "Homeland security and homeland defence outlook 2006-2015]

2.5.2 Homeland Security forecast by application area

Figure 6 outlines the forecasted Homeland Security market using the segmentation discussed in Section 2.2. It should be noted that in the market forecast, airport, land border and seaport segments have been combined into an entry point and transportation security segment. This is a common approach and mirrors the organisational structure of the government departments and related budgetary segmentation. The Homeland security market is dominated by border and transportation security and infrastructure protection comprising of 40% and 21% in 2006 respectively. Chemical, biological, radiological and nuclear (CBRN) security is a significant and high growth area contained within the border and transportation security and infrastructure protection segments. It has therefore been explicitly split from these segments.

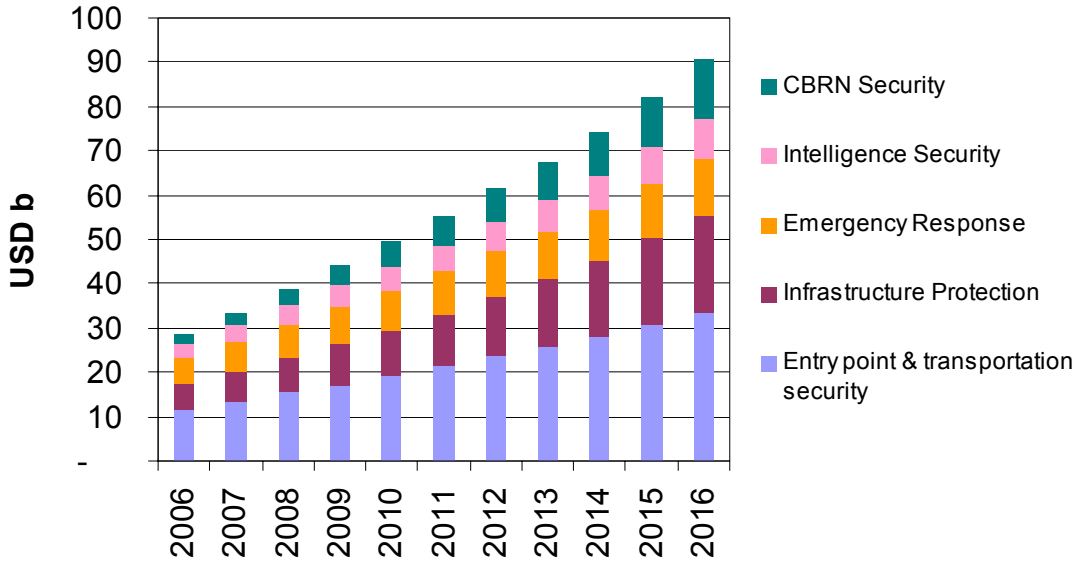


Figure 6: Homeland security market forecast (2006-2016) by application area [Source: ITI Techmedia, Initial data taken from HSRC report "Homeland security and homeland defence outlook 2006-2015]

3 MARKET OPPORTUNITY ASSESSMENT

This section describes 11 specific market opportunities within the Homeland Security space, and sets out the process by which they were identified.

3.1 Introduction

Within the six high level market segments previously defined, 30 areas of market opportunity were identified where unmet needs might exist. This was done on the basis of secondary research data, including market analyst reports, industry comment, published government information and public domain company information. This data allowed a segmentation matrix to be created, mapping specific areas of technology function to areas within Homeland Security market segments. This mapping was consolidated into 30 specific opportunities covering the Homeland Security market space.

The resulting opportunities were then developed and assessed through a programme of primary research, including interviews with market participants (both public and private sector) and two half-day workshops held with leading companies active in the sector along with representation from the public sector concerned with national security. The interviews were used to develop the opportunities in terms of unmet needs and market requirements within each opportunity area. The most interesting areas were then discussed in the workshops sessions, which provided insights into the key areas of development which were viewed as likely to be of interest from a market viewpoint within the next 3-5 years.

This process provided a mechanism for ranking the identified opportunity areas in terms of the following criteria: addressable market size, unmet market needs, degree of technical risk involved in addressing the opportunity, ability of anticipated solutions to meet market needs and potential market window (timescale for significant market development). In turn, this allowed the areas of maximum opportunity for technology platform development to be identified.

The rest of this section outlines in detail the top 11 opportunities which were identified following which the remainder of the opportunities (which were not progressed) are briefly discussed.

3.2 Description of Top Market Opportunities

The workshops highlighted several areas of national importance where unmet needs exist which, due to the technical difficulty involved in making the significant developments required in these areas, are unlikely to be resolved in the short term. Therefore these areas represent important opportunities for the creation of valuable IP which can be commercialised within the ITI market opportunity timeframe (3-10 years). In addition, the workshops identified additional areas where Homeland Security spending to date has been limited (because for example no significant terrorist event has yet occurred), but where security concern has risen to the point where significantly more spending in these areas is possible over the next few years. These areas are also included in the list of opportunities selected.

The opportunities are:

Opportunity	***Summary***
Explosives detection	Detection systems for explosives at airports, border crossings and critical infrastructure sites
Airport perimeter security	Security systems to protect airport perimeters
Video analytics	Recognition of individuals and objects from video data
CCTV	Intelligent CCTV systems integrated with sensor and surveillance systems

Opportunity	***Summary***
Biometrics: Face recognition	Authentication of individuals and other security applications from imaging data
Border monitoring and control	Integrated sensor, surveillance and intelligence systems for border monitoring
Data analysis and threat detection via intelligent data mining	Identification of threats via the intelligent analysis of huge amounts of data from a range of different sources (including personal data) to determine correlations and patterns which are likely to be important for Homeland Security investigations
Freight container security - monitoring and tracking	Monitoring and tracking of freight containers at seaports and border transit points
Effective threat detection based on data fusion and domain-specific threat modelling and analysis	Threat detection based on the integration and analysis of data from a range of security sensor networks and domain-specific threat modelling and analysis to enable the discrimination of genuine threat indicators from behaviours which are benign
Vulnerability assessment	Applications for risk assessment and vulnerability analysis for protection of critical infrastructure
Information intelligence – privacy and security controls	The proactive gathering, analysis and dissemination of information on potential security threats within a framework which retains the security and privacy of the underpinning data

Figure 7: Top Homeland Security market opportunities [Source: ITI Techmedia]

These opportunity areas are likely to be subject to the same ecosystem constraints described previously. However it is likely that successful developments will also lead to significant commercial opportunities for the technology, which in many cases will provide revenue opportunities.

Each of these opportunity areas is described further in the following sections. For each opportunity the following is provided:

- What is it?
- What application does it enable?
- Market and ecosystem
- What are the unmet needs?
- Market size
- Market barriers and enablers
- Timescale (market window)
- Key players
- Conclusion

3.3 Explosives Detection

What is it?

Effective detection systems for individuals carrying explosives are required at key transit/access points, including airports, border crossings and critical infrastructure sites. Traditional bulk detection systems (typically based on X-ray imaging) have proved to be not efficient enough (e.g. passenger throughput is too slow), and have proved expensive and prone to false alarms. A wide range of technologies has been deployed to provide specific detection of explosives, but so far cost, reliability and throughput requirements have not been met.

What application does it enable?

Explosives detection is relevant for many security areas, and efficient, reliable, cost-effective detection would see widespread application, for example at:

- Airports – trace detection of explosives (incl. Improvised Explosive Devices) for passengers, carry-on and checked bags and air cargo
- Military installations – screening at entry points
- Power plants, government buildings – screening at entry points
- Rail and underground stations – passenger screening
- Large events/stadia – entry screening

The vision is of a reliable, cost-effective sensor system which can provide detection of trace levels of explosives with very low false alarm rates and minimal impact on passenger or cargo throughput.

The reality is current explosive detector systems require a manual operation (and hence are expensive and screen only a low percentage of passengers), bulk detectors are expensive to install and maintain and walkthrough portals (e.g. puffer systems) have proved unreliable due to dust and dirt in the airport environment.

The next step is the emergence of a robust, “real-world” system which can detect “suspicious” traces reliably at low cost and with low false alarm rates. Explosives sensors are likely to provide information into a threat detection system which uses other information sources and knowledge of current threats to provide robust alerts to system operators. Integration of explosives sensor data into an intelligent threat analysis network is a key part of this.

Market and ecosystem

Many companies have developed explosives detection systems based on a range of approaches and technologies, including particle/vapour (puffer) systems, finger touch systems, low frequency micro-waves, Computed Tomography (CT) imaging, terahertz imaging, neutron activation and nuclear quadrupole resonance. To date, a winning solution at the system (not component) level has not emerged.

The market is defined by government spending (e.g. on airport systems), and hence is addressed by major security companies such as GE InVision and L-3 (who dominate checked baggage) and GE and Smiths Detection (who lead in people screening). There are many new entrants and approaches made by smaller companies in this market but market entry is difficult in the absence of a clearly compelling solution.

What are the unmet needs?

- A cost-effective, automated, in-line screening process for people and carry-on luggage – e.g. a walk-through trace portal – which is better than an experienced security person
- Capability to detect liquid/paste explosives (X-rays don’t discriminate liquids); liquids may not have been handled by their carrier
- Ability to detect smaller quantities of explosives and explosives in different locations on the body (e.g. in shoes)
- Reliable systems with affordable installation and maintenance
- Rapid scanning of air cargo – less bulky machines are needed
- Reliable and inexpensive handheld detectors
- Cheaper, rapid throughput solutions for ports and mass-transit stations
- Effective downstream methods to identify what the explosive is
- Critically, low false alarm rates

Market size

The US market for explosives detection equipment is estimated at USD1.6 billion 2007-2009, the European market EUR 325 million in 2010 (Source: Frost & Sullivan). US airports were equipped with screening systems in 2004, at a cost of ca. USD1m/unit.

Market barriers and enablers

- Drivers and Enablers
  - Increased threat from improvised explosives on transport systems
  - Raised awareness of the threat from liquid explosives or explosive precursors carried on to aircraft
  - Extensive development activity on explosives detection for airports
- Barriers
  - Specific technology development barriers, e.g. lack of inexpensive terahertz radiation sources of the right form factor
  - Lack of a 'library' of spectrum fingerprints for different explosives
  - Limits on government spending in this area

Timescale (market window)

Depending on developments in reduced cost and more reliable systems, spending on carry-on baggage screening at airports could increase from 2007, followed by spending from 2008 on trace portals/body scanners and on air cargo screening. This could open up wider markets for screening systems in ground transportation and at events around 2010.

Key players

Leading players in this market and smaller companies developing interesting technologies include:

Leading players:

- GE InVision: http://www.gesecurity.com - Market leader in screening technologies
- L-3 Communications: http://www.l-3com.com/ - Market leader in screening technologies, including bulk detection of checked luggage
- Selex Sensors and Airborne Systems: http://www.selex-sas.com/about_sas.html - Leading sensor solutions company
- Smiths Detection: http://www.smithsdetection.com/ - Market leader in screening technologies

Technology specialists:

- QinetiQ: http://www.qinetiq.com/ - Explosive detection using passive millimetre wave sensing
- M Squared Lasers: http://www.m2lasers.com/ - Solid-state laser products, e.g. high brightness terahertz laser source
- Owlstone: http://www.owlstonenanotech.com/ - Nanofabrication detection technology
- Reveal Imaging: http://www.revealimaging.com/ - Explosives detection integrated into airport flow
- Iconal Technology: http://www.iconal.com/ - Use of terahertz and millimetre wave technology for security

Conclusion

The explosives detection market is large and encompasses a wide range of potential deployment areas. Unmet needs revolve around the development of a cost-effective, robust and practical system which can detect a wide range of explosive types/locations. Terahertz is an interesting candidate technology, but real-world systems based on terahertz which fully meet

user requirements have not yet been developed. Integration of data from explosives sensors into an intelligent threat analysis network is an interesting component of likely future systems.

3.4 Airport Perimeter Security

What is it?

Security systems to protect airport perimeters (i.e. fenced perimeters away from passenger, staff and goods access points) are a significant growth market. Airport perimeters are extremely long and, in addition to significant new airport build in Asia, there is growing concern about strengthening perimeter protection at existing airports to prevent intrusion into the airport and deployment of weapons against planes. As passenger security procedures are tightened, vulnerability may migrate to the perimeters.

What application does it enable?

In addition to airports, industrial installations such as power stations (private utilities in the US) have lengthy borders which need to be protected.

The vision is that as security concern migrates to airport perimeters, more sophisticated and automated systems will be required to secure the perimeters effectively. These will have more scope to include new technology in the design, as the cost of the manpower required will need to be reduced.

The reality is that current airport perimeters can be porous, particularly for airports outside the top tier, as they may rely mainly on physical barriers. This has important implications for security risks.

The next step is the development of a robust system which can detect suspicious activity reliably and with low false alarm rates. This should have a high degree of automation allowing manpower cost savings.

Market and ecosystem

Airport perimeter security consists of physical barriers, sensors and command and control systems. As well as (physical) fencing to keep out deliberate and accidental intruders (e.g. animals), sensor systems, for example radar and pressure and acoustic sensors (which detects cut fences), are used to detect threats. CCTV and video analytics may be deployed to determine individuals who may pose a threat. Command, control and communications systems (C3) are used to co-ordinate detection and response. Novel approaches – e.g. lightly buried fibre optics sensitive to pressure changes – could be incorporated into such systems. The airport perimeter security market comprises multinationals, system integrators and smaller niche companies.

What are the unmet needs?

- Effective integration of systems from different vendors, customised to each airport's needs
- Support for legacy systems (e.g. installed analogue CCTV systems) in a changeover period where new technology must work alongside deployed solutions
- Protection of planes against modern weapons, e.g. rocket-propelled grenades , man-portable missiles
- Ability to cope with poor weather conditions, reliable, low maintenance
- Reduce manpower costs by fewer false alerts

Market size

Airport perimeter security markets are very large, estimated at USD3500 million in 2006, rising to USD7400 million in 2011 (source: Frost & Sullivan). Total spend from 2006 to 2011 is estimated at USD33 billion worldwide, split equally into physical barriers, sensors, and

command and control systems. Growth is driven by new airport build, e.g. in Asia, where greater opportunities for technology-based solutions may exist.

Market barriers and enablers

- Drivers and Enablers
  - Market likely to be driven by government policy and standards
  - Increasing awareness of perimeter security issues
  - New airport build; re-equipping existing airports
- Barriers
  - Governments may not set appropriate standards, or provide the required funding
  - Concern about airport perimeter security is not necessarily rational, e.g. perimeters do not protect against missiles
  - Increasing manpower may be more cost-effective in the short term

Timescale (market window)

Analysts predict strong growth from 2006 as needs become more accurately defined and budgets become available. More emphasis is starting to be placed on perimeter security (previously emphasis was placed on baggage and terminal protection) – this is likely to boost demand in the medium term.

Key players

Leading players in this market include companies providing solutions for perimeter control applications:

- ADT Security Services: http://www.adt.com/ - intrusion detection, control and surveillance systems
- FLIR Systems: http://www.flir.com/ -Thermal and multi-sensor imaging systems for land-based applications
- Magal Security Systems: http://www.magal-ssl.com/ - Perimeter intrusion detection using a range of technologies

Conclusion

Airport perimeter security is a large and growing market – significant opportunities are likely to develop for companies who can integrate technology developments into effective surveillance and security systems which provide return on investment through (for example) manpower cost savings. There is scope for developing innovative approaches for airport perimeter security to complement or replace current approaches.

3.5 Video Analytics

What is it?

Video analytics covers the recognition of individuals and objects which pose a threat or require attention from video data. Huge growth in the deployment of CCTV cameras and the amount of video data recorded is overwhelming the manual capacity to search this data. Automated methods for identifying individuals and objects in video data are required. The need for this is high, but market development depends on the performance which can be achieved.

What application does it enable?

Effective video analytics are likely to be part of solutions which combine security factors from a range of different sources, for example motion detection, object detection, perimeter protection, target tracking etc. Important capabilities are to identify entities of interest in real time, process efficiently vast amounts of video from spiralling numbers of image sensors (post event search), track entities from scene to scene and present actionable information to end users instead of simply presenting operators with the video data.

Intelligent analysis is required, for example to identify people entering a station with bags and then leaving without them, or deduction of potential incidents (e.g. abandoned cars as potential bombs).

Wider applications include for example video management of archives, security applications in banking and financial services and analysis of customer behaviour in supermarkets.

The vision is of a video analysis system which correctly targets suspicious individuals, behaviours and objects in real time from video data streams, correlate entities across multiple camera views (camera handover) and recorded data, and provides operators with alerts and rapidly generates lines of enquiry.

The reality is that current capability in this field does not yet meet the requirements. Finding a target automatically in CCTV in real time is a very hard problem. Although some success has been achieved in identifying distinctive patterns (e.g. brand logos) from video data, further performance improvement is needed.

The next step is further development to increase performance of video analytics to meet Homeland Security requirements, particularly in terms of current Homeland Security needs to pick out security-relevant data from images and track people and objects across multiple scenes.

Market and ecosystem

The emerging video analytics ecosystem comprises a number of technical specialist developers. Often they are developing commercial applications in parallel with work on Homeland Security systems – it may be that problems are solved first in the commercial space and then applied to public sector security applications.

What are the unmet needs?

- Improved performance – current intelligent video processing systems are still some way from being practical and reliable other than some basic systems
- Reduced costs per install – equipment costs are currently high and installation is complex
- Methods for correctly picking out useful data
- Lack of standards for information exchange
- Effective camera handover – tracking people/objects across multiple cameras
- Effective scene interpretation and behaviour analysis (accurate identification of threats based on analysis of people's behaviour in video data)
- Analytics for: mining of "archaeological" data; identification from a watch list; activity scanning

Market size

The video analytics market is estimated at USD60 million in 2005, rising to USD416 million by 2012 (source: Frost & Sullivan). This could be a conservative view – analytics are likely to be a component in many video systems if performance can be improved sufficiently.

Market barriers and enablers

- Drivers and Enablers
  - Increasing deployment of IP-CCTV systems which allow control of the quality of captured video data
  - Potential to improve the performance of operatives analysing historic data and hence reduce manpower costs or extract useful information from data which would otherwise not be analysed
  - Drive to reduce the amount of manual intervention and supervision required for real-time, multi-camera surveillance systems due to video information overload

- Barriers
  - Current performance does not meet Homeland Security requirements (as defined in unmet needs)
  - Performance on test data or under controlled conditions can be good, but current systems often fail under real world conditions
  - False alarm rates are unacceptably high

Timescale (market window)

Timescales for deployment are unclear, as this depends on solving the performance issues. However given the high current level of activity in this area, it is likely that significant improvements will be made in the short to medium term.

Key players

Leading players in this market include a range of companies developing video analysis solutions, including:

- OmniPerception: http://www.omniperception.com/ - Solutions for automatic identification from video data, including commercial and surveillance applications
- Verint Systems: http://www.verint.com/ - Extracting intelligence from video data
- Waterfall Solutions: http://www.waterfallsolutions.co.uk/ - Image processing for military and commercial applications

Conclusion

Video analytics presents a strong opportunity in security markets, with several critical unmet needs from a Homeland Security viewpoint. Strong commercial applications are also evident; these may be realised prior to application in security-related areas. However the technical challenge is considerable.

3.6 CCTV

What is it?

The move to digital (IP-based) CCTV systems enables the development of intelligent CCTV systems which can be integrated with other security data sources and security applications. This offers the potential for significant improvements in automation and threat detection, and much lower false alarm rates. As the deployed base of legacy analogue systems is replaced, this market should offer significant potential.

What application does it enable?

Intelligent CCTV surveillance integrated with sensors, biometrics (e.g. face recognition) and access control data (e.g. from access RFID tags) has the potential to provide security applications with a dramatic improvement on current false alarm rates (which can be up to 90%). Applications include preventing entry of terrorists, crime detection and prevention, industrial security in chemical or power plants (for example) and in domestic security.

The vision is of an intelligent IP-CCTV system which automatically controls, analyses, correlates and stores appropriately high volumes of video and other security data without detailed operator intervention.

The reality is that although the benefits are clear (for example even trained observers lose focus after 30 minutes) it is hard to make such systems work. Current CCTV systems rarely detect real threats before the event.

The next step is the development of intelligent analysis, compression and storage for CCTV systems combined with fusion with other security data. This would be good feature widely applicable to many Homeland Security applications.

Market and ecosystem

The CCTV ecosystem ranges from camera developers and manufacturers to installers of basic systems. Recently more specialist providers of more advanced IP-CCTV systems have seen significant growth, into segments such as town centre deterrence and systems for high end intelligence.

What are the unmet needs?

- Constantly scanning camera data translated into real-time alerts without the need for cooperative subjects
- Effective integration with security-based video analytics, for example human behaviour analysis (e.g. pinpointing distress in a crowd) or person/object recognition
- Real world systems not components
- Effective outdoors and in poor lighting conditions
- Low false alarm rates
- Protection of the evidence value of archived CCTV footage – appropriate storage, retention and integrity, and maintenance of timelines

Market size

Whilst a significant market for small, cheap CCTV cameras exists, growth is also being experienced in advanced CCTV segments such as security systems deployed in urban areas. For example the UK CCTV market alone is forecast to reach £384 million in 2007 (source: Frost & Sullivan).

Market barriers and enablers

- Drivers and Enablers
  - Requirement for systems which capture and store “interesting” video data at high quality
  - Drive towards data fusion (analysing and acting on security data drawn from a range of different sources)
  - Availability of high end, networked cameras at reasonable cost
- Barriers
  - Little drive to replace analogue systems in many cases
  - UK market for basic systems saturated, prices falling
  - Privacy issues for advanced CCTV systems are a significant concern

Timescale (market window)

Although the advanced CCTV market has shown rapid recent growth, incorporating more complex intelligence and analytics into CCTV infrastructures is likely to take some time. However, user demand and the presence of many companies working in this area are likely to provide significant momentum for the market in the medium term.

Key players

Leading players in this market include:

- Axis Communications: http://www.axis.com/ - Provider of networked-video solutions
- CoVi Technologies: http://www.covitechnologies.com/ - High-definition video surveillance systems
- Indigovision: http://www.indigovision.com/ - Provider of IP-based CCTV systems
- ObjectVideo: http://www.objectvideo.com/industry/homeland/ - Intelligent video on a chip market leader
- Quadnetics: http://www.quadnetics.com/ - Advanced surveillance technology and security networks

Conclusion

Significant potential exists for the development of CCTV systems which effectively implement the security applications required by government. High added-value development is likely to focus on embedding effective analytics and intelligence applications within camera and storage control systems.

3.7 Biometrics: Face Recognition

What is it?

The use of face recognition biometrics is designed to enable the authentication of individuals from imaging data. This is a very challenging task – whilst the biometric is non-contact and non-invasive, currently close range is required which limits the application of the method. A range of approaches to the problem are being tried, including mapping unique vascular patterns using 3D IR imaging, using stereoscopic cameras for 3D face mapping and using melanin structure biometrics.

What application does it enable?

Effective face recognition would enable a wide range of security applications, for example authenticating individuals against a template, searching a live data stream against watch-list, and integration of face recognition data into "smart surveillance" applications. This could be used in a wide range of situations:

- Passport systems: comparison with a watch list
- Personal ID systems: drivers licences, visas
- Access control: doors, gates (e.g. at airports)
- Casinos: detecting unlicenced users
- Allowing access to health records
- Police: comparison of monitoring data with 2D image databases

The vision is an automated face recognition system which delivers authentication with accuracy, scalability, speed and convenience. Ideally the system should deal with challenging conditions, for example emergency evacuations, disguises, twins, impersonators, darkness.

The reality is that this remains a big technical challenge; performance improvements are required for one to one authentication using face recognition.

The next step could be developments in potentially disruptive technologies, for example vascular pattern recognition.

Market and ecosystem

The market for face recognition is driven almost entirely by government's desire to introduce new regulations for ID purposes. Non-government applications are a small fraction of overall market.

What are the unmet needs?

- Robust, cost-effective, "real-world" systems
- Newer 3D algorithms, as opposed to the current 2D algorithms, may give relaxation on image capture requirements
- Systems which deal effectively with recognition problems, e.g. aging, different ethnic origin
- Cost-effective enrolment, i.e. a system to capture a database of facial information of a population against which an individual's face biometric can be authenticated
- Disguise detection, i.e. a system which can detect the identity of an individual who has disguised themselves

Market size

Effective 3D face recognition is likely to command a substantial market. For example, the market is projected to rise from USD186 million in 2005 to USD1021 million in 2012. However, cost is a barrier in moving to 3D systems and there is likely to be strong competition from other biometrics, which may be cheaper. Existing players in the market are constantly improving, and hence this is a maturing technology.

Market barriers and enablers

- Drivers and Enablers
  - Operationally simpler to use than iris or fingerprint
  - Suitable for "walk-by", i.e. replacing the passport queue
  - Face recognition is robust against impostors (attempts to use another person's identity)
  - Supports visual inspection and compatible with legacy verification methods
- Barriers
  - Constraints on overall system cost
  - High system engineering requirements
  - The need for high resolution image capture
  - Constraints may restrict accuracy if implementation is poor
  - Competition from mature biometrics, e.g. iris recognition
  - Current systems not effective against people who wish to disguise themselves

Timescale (market window)

The market is starting now in the UK, driven by regulation, and is likely to grow through to 2014 (deployment at high security facilities).

Key players

Leading players in the face recognition market include:

- A4Vision (Bioscrypt): http://www.a4vision.com/ - Real-time 3D facial recognition and matching
- Cognitec: http://www.cognitec-systems.de/ - Face recognition software and technology
- Geometrix (Alive Tech): http://www.geometrix.com/ - Multi-biometric technology blending 3D face, 2D face, and fingerprint
- L1 Identity Solutions: http://www.l1id.com/ - Live scan systems and services for biometric data capture, mobile solutions for on-the-spot ID and facial screening

Conclusion

A face recognition system which is effective in "walk-by" (i.e. not just close range) situations would find use in a number of significant government-driven security applications, and could command a substantial market. Existing approaches have not yet delivered the required performance in real-world applications, and there is scope for looking at innovative approaches to address this problem.

3.8 Border Monitoring and Control

What is it?

Integrated sensor, surveillance and intelligence systems deployed at borders and border crossing points for the detection of terrorists, explosives, narcotics and other undesirable individuals and substances. Extensive national land and sea borders are difficult to monitor and control. Whilst technology-based solutions have been tried (particularly in the US), these have been expensive and prone to high false alarm rates. Cost-effective systems are required which integrate border surveillance information with intelligence data to provide agents with reliable and actionable detection of suspicious activity.

What application does it enable?

Provision of “actionable intelligence” to border control agents would find application in a variety of border areas:

- Land border patrol – prevent the entry of terrorists, nuclear material, explosives, drugs, illegal immigrants etc.
- Sea border (coastline) patrol – prevent illegal craft landing
- Military applications – tactical awareness, command and control.

The vision is of an integrated network of low maintenance surveillance devices (e.g. long range cameras, seismic sensors, patrol radar, X-ray cargo scanners etc.) integrated into an IT infrastructure which translates the data gathered from field assets into an actionable response to real threats.

The reality is that current systems are not sufficiently integrated and do not meet end user (e.g. patrol agent) needs. With current systems false alarm rates are high as (for example) cameras are not linked to sensors (to reduce time wasting false alarms).

The next step is to demonstrate appropriate detector systems which are integrated with threat analysis and intelligence data to provide effective support systems for border patrol agents.

Market and ecosystem

Border monitoring and control systems are procured by governments, particularly in the Middle East, and where there are long land borders (e.g. the US). Trial deployments in the US (covering land borders and coastlines) have proved expensive and have highlighted significant performance issues with the deployed systems. Whilst the heavyweight security companies such as General Dynamics, Lockheed Martin and Northrop Grumman are likely to compete in this market, opportunities may exist for specialist technology suppliers to these companies.

What are the unmet needs?

- Linked sensor/video surveillance capability
- Interoperability between border control systems
- IT systems which provide “actionable intelligence” not overwhelming data
- Effective surveillance cameras – IR, night vision, motion detection, all weather, facial recognition capability with high degree of certainty
- Self-powered sensors which can stand extreme environments and provide low false alarm rates e.g. don’t alert for animals
- Scalability – smugglers overwhelm the system's vulnerable points with large numbers of simultaneous illegal border-crossers

Market size

This has been a “hot button” issue in the US, with a US market size of USD1.2 billion in 2006 (source: Frost & Sullivan). The market is growing, particularly in terms of: surveillance, biometrics, IT systems (which is the largest segment), air assets (manned and UAVs), sensors and detection equipment.

Market barriers and enablers

- Drivers and Enablers
  - EU accession country borders may attract EU funding for border protection
  - Growing awareness of the importance of preventing illegal boats reaching the US coastline, which is largely unprotected
  - Increasing importance of land border security in the Middle East
- Barriers
  - Impact of high false alarm rates, which can dwarf the real threats

- Recognition that US technology-based border protection initiatives in the last 10 years have largely failed
- Currently more emphasis is being given to proven solutions – more officers, trained dogs
- The high cost of full protection, e.g. protecting the entire US land border is impractical

Timescale (market window)

Steady growth in this market is forecast through to 2010 in the US, as Homeland Security spending covers the most significant border vulnerabilities. Awareness of the importance of port security is increasing.

Key players

Leading players in the market for national border security comprise major defence companies, for example:

- General Dynamics: www.gd-ais.com - Border security intelligence, surveillance and reconnaissance
- Northrop Grumman: www.is.northropgrumman.com - Integrated surveillance and reconnaissance systems
- Raytheon: www.raytheon.co.uk/products/homeland_security.html - Border control programmes
- SAIC: www.saic.com - Homeland security solutions for the (US) DHS
- Selex Sensors and Airborne Systems: http://www.selex-sas.com/about_sas.html - Leading sensor solutions and border security company

Conclusion

A need exists for detector systems which are integrated with threat analysis methods and intelligence data sources to provide effective support systems for border patrol agents. The provision of actionable intelligence with low false alarm rates by systems which correlate and control data from different sources would provide a step change in surveillance capability across land and sea borders.

3.9 Data Analysis and Threat Detection via Intelligent Data Mining

What is it?

It has been cited that the perpetrators of 9/11 left an audit trail of information that was known to the security authorities and if effectively correlated could have provided the intelligence to prevent the attacks. Only hindsight offers the luxury of tracing the information associated with known perpetrators. The most effective current intelligence models are based on association based data search. This is well known to terrorists who will use methods of recruitment and engagement that are based on difficult to detect associations.

The real challenge to intelligence activities is to create foresighting capabilities that can detect terrorist patterns where the suspects emerge from bottom up analysis rather than the more restrictive search that is enabled using guilt by association. Inevitably this means enabling threat detection based on performing data analysis of huge volumes of personal information data, where everybody is a potential suspect.

Note that there are separate challenges to be addressed, one of which is the duty of care of protection of privacy within a system that invades that privacy by design. This opportunity is specific to the challenges relating to synthesis and escalated visibility of relevant intelligence. Privacy and security issues relating to the protection of the data itself is addressed separately.

What application does it enable?

Effective counter terrorist intelligence and threat identification that is not dependent on tracing.

The vision – and its attendant problems – is perhaps best described by the name initially attached to this in the US, which was *Total Information Awareness (TIA)*, launched by the Pentagon in 2002. The system should be a self-configuring intelligence monitor that intelligently selects between alternative algorithms and reasons about other relevant information that should be investigated. Whilst the top level system is necessarily held under government control there should be an ecosystem for competitive provision of new primary and secondary analysis tools that support rich data-mining functions to provide initial detection.

The reality – The Office of the Director of National Intelligence "is building a computerized system"—called Tangram—"to search very large stores of information for patterns of activity that look like terrorist planning". Sources of analysed information include:

- aggregate suspicion scores based on guilt by association algorithms
- government intelligence databases
- private communications
- financial transactions
- web access behaviours.

Announced in Oct 2006, and with its official status is as a research and development program, the initiative has drawn similar levels of criticism and privacy concerns that caused the original TIA program to be converted into a classified R&D program. In addition:

- The Trusted information Network and Information Sharing and Analysis Centres (ISACS): collate and analyse data at the Homeland Security Operations Centre, where aggregate data can be searched and analysed within an integrated intelligence hub
- The eBorders program within the UK gathers and analyses inbound passenger information
- The SafePassage program from TSA (Transport Security Association) collects and monitors passenger information.

It is conceivable that programs such as Tangram will enable significant advances in the analysis capabilities that can address large disparate data sets. However, the low key manner in which these programs engage with suppliers may imply that there is a market defect in respect of best possible provision of viable solutions[3].

The next step – The nature of market engagement makes it difficult to be prescriptive about the tactical steps for generation of a technology to address this problem. ITTs issued by the Directorate of National Intelligence suggest that the algorithms are secure and the residual problem is the application of these algorithms in scale.

However, reports on the actual performance within Tangram suggest that the fundamentals of enabling algorithms to address the scale of data to be analysed have not been properly considered. This may indicate that the optimal approach to addressing scalability may be algorithm independent, or conversely a more abstract framework that can exploit different algorithms applied in combination.

The underling problem is that the number of potential relationships that exist in a database grow rapidly and exponentially with the volume of data present. In order to get anything close to linear scalability, which is pre-requisite for a practical real world solution, then some level of information compression or filtering must be applicable based on a hierarchical segmented approach to the data sources. This problem is potentially very difficult to address since

[3] For example the main suppliers for Tangram R&D are effectively the same players who were involved in the TIA initiative in 2002

segmented approaches to data analysis run the danger of losing discovery of important anomalies that are contingent on correlated access to the primary raw data.

Providers vary in the importance they attach to filtering or compression of the raw data. It may be reasonable however to assume that an effective solution must use initial filtering for first order search, but then selectively explore the expanded data-sets based on a reduced number of suspects that are uncovered from the first order analysis.

A possible next step therefore may be to look towards academia or companies already active in security related data-mining, to identify potential technical approaches to addressing the scalability issue, and use these as the basis for constructing an analysis work bench that supports coordination of a variety of algorithmic approaches.

Market and ecosystem

The current market for this kind of technology is via direct engagement with the Office of the Director of National Intelligence in the US and the Home Office Scientific Development branch in the UK. There are no public statements of requirements and in the US in particular there are perceived political tensions and opposing agendas as to the manner in which such programs get funded, if at all. Current indications are that the US is likely to circumvent privacy concerns through lack of transparency, and paradoxically may therefore inflame such concerns, whilst in Europe there is much more likely to be a higher level of attention to societal and political dimensions of information surveillance on the ordinary population.

What are the unmet needs?

- Data analysis and mining on this scale has never been done before and poses huge challenges
- TIA is an ideal, which requires exploring and scoring of every potential association. However such a search space grows exponentially and rapidly. It is not addressable unless strategies for information compression, splitting and refining of search spaces are applied. Current mechanisms for doing this are based on crude filtering against local anomalies and threat signatures. Premature filtering leads to non-discoverable links which can be exploited to retain low visibility
- The exploiters of this technology have a need to keep the knowledge base of threat patterns secret. This can limit the focus of R&D, and sets challenges for the separation between analysis engines and more specific analysis rules used for inference
- Performance requirements of large scale data-mining are cripplingly high, related to the processing load that is necessary for bottom up discovery analysis.

Market size

Initial US Government spending in Tangram is of the order of USD50 million for initial R&D. Total funding for this market is believed to be in excess of USD1 billion per annum in the US alone, based on an indicator figure of market spend of USD700,000 in 2005. Future market projections are very sensitive to market uncertainties relating to public acceptance of the perceived invasion of privacy. HOSDB have given very strong indications that the same market need exists in the UK, but that within Europe as a whole the development of privacy protection measures would need to be much more mature.

Market barriers and enablers

- Drivers and Enablers
  - Developments in key enabling technologies, for example in data mining, data aggregation, data fusion and algorithm fusion technologies
  - Effective hierarchical filtering and information compression to support scalability over various dimensions including number of people and modes of monitoring
  - Reasoning and analysis systems for inference of behaviours such as terrorist planning activity

- Barriers
  - Lack of openness in market engagement
  - Privacy concerns and suspicion of government agendas
  - Practical issues of ensuring ongoing access to large sources of data
  - Exponential nature of potential associations or correlations required for deep data mining

Timescale (market window)

The market currently exists but is difficult to quantify, and subject to tentative growth. It is arguable that high growth will not occur until such time that the conflicting needs of privacy protection and public safety find some level of mutual accommodation.

Key players

Leading players in this market include:

- 21st Century Technologies: http://www.21technologies.com - Network analysis (SNA) and graph matching as methods for finding patterns and anomalies
- ArcSight: http://www.arcsight.com/ - Provision of security and compliance intelligence by identifying, prioritizing and responding to security threats and network changes
- Memex: http://www.memex.co.uk/ - Intelligence management software solutions
- SRI Technologies: http://www.sri.com/ - Independent, non-profit research institute conducting research in information analysis

Conclusion

The market for threat detection based on deep data mining is potentially very large, but is subject to significant uncertainty due to the importance different governments will give to privacy concerns. Whilst it is possible that processing performance improvements may have some impact on the problem, it is more likely that significant improvements in the algorithms used or in the way in which the problem is structured and addressed will be required to achieve the level of performance which will meet the market need.

3.10 Freight Container Security - Monitoring and Tracking

What is it?

Freight container security covers the monitoring and tracking of freight containers at seaports and border transit points. The required technology elements exist, and the needs are recognised, but an effective market is not yet in place to enable procurement. Solutions are required which improve operating efficiency and provide benefits to goods owners and shippers as well as ensuring security.

What application does it enable?

Freight container security systems aim to guarantee the integrity of shipments by providing tracking (typically based on RFID), tamper monitoring functions (ensuring that containers sealed with anti-tamper technologies have not been breached) and condition monitoring functions (recording the conditions experienced by the container contents during transit). This can be done on behalf of a government to achieve its objectives for security, or by companies who fund the introduction of appropriate RFID security/logistics systems on their container shipments for business reasons – brand protection is one of the main reasons for validation of shipped goods in this way. More advanced implementations are possible, for example PKI based pre-certification of shipments using digitally signed high capacity RFID memory tags.

The vision is of a ubiquitous, low cost, standards-based system which ensures container security and improves supply logistics.

The reality is that RFID systems using active tags which monitor a container's internal environment, conditions experienced and check for opening/tampering en route cost ca. USD10-20 per container. Since the costs of damage resulting from dangerous shipments are not borne by those who would need to pay for the system, there is no direct incentive for shippers or port operators to bear this cost. Most systems are therefore based on identifying high risk containers at foreign ports and checking these on entry. Thus, large numbers of containers are never checked.

The next step is likely to be the introduction of requirements to track shipments which fit specific risk profiles, together with a cost structure that reflects the status of the container operator and of the goods owner. Systems would need to be cheap enough and reliable enough to make this work.

Market and ecosystem

Initiatives in this market have been taken by port operators and commercial goods owners, drawing on the wider RFID market. No urgency is yet set by the wider market (i.e. governments), but this could change if, for example, a major terrorist incident occurs involving this route.

What are the unmet needs?

- A system which enables higher security for the import of containers that avoids the need for disproportionate cost to be absorbed by sea port
- Need to contribute to improvements in supply chain efficiency to justify the cost
- Integrated capability to detect hazardous materials (cargo screening) – such systems need to be robust, easy to install and capable of surviving conditions at sea
- Scale and implementation issues need to be addressed (e.g. trust/regulation/interoperability), however these may not be require technology-based solutions
- A trust infrastructure required to enable targeted inspections at port of entry

Market size

Market size projections based on current levels of government spend in this area are relatively small, e.g. the European market could reach EUR 150 million in 2010 (source: Frost & Sullivan). However for example the US market size could reach USD1.5 billion if the enormous implementation cost can be justified.

Market barriers and enablers

- Drivers and Enablers
  - Growing awareness that shipping containers (potentially containing explosives, drugs, arms or nuclear material) is the biggest security hole (current level of screening at US ports of entry is very low (5-6%))
  - Innovative business models are possible, e.g. subsidised or free tags and a pay per use system for access to a secure data network
  - Where the cost of inspection is sensitive to the required security level, differential tariffs could be applied, which would provide an incentive for carriers
- Barriers
  - Interoperability between different systems – shipping/port and scanning companies need to agree appropriate standards
  - High volume adoption is essential to justify the system cost
  - Sea ports cannot bear the cost of the required security (shippers generate only a small profit per container)
  - No international agreement about who bears responsibility for dangerous shipments

Timescale (market window)

The market is likely to see steady spending from 2007 through to 2014. Significant take-up is likely to be 2008/2009, based on current spending patterns.

Key players

Leading players in this market include:

- Datamars: http://www.datamars.com/ - RFID solutions for a range of markets
- Hutchison Port Holdings: http://www.hph.com/ - Port operations and related services
- Intermec Technologies: http://www.intermec.com/ - RFID solutions for a range of markets
- Savi Technology: http://www.savi.com/ - RFID solutions covering consignment and shipment management, and global supply chain visibility and security
- TI RFID systems: http://www.ti.com/rfid/ - RFID technology and manufacture

Conclusion

There is acknowledgement that unscreened shipping containers present the biggest hole in national security systems. Whilst the technology exists to plug this gap this is currently not generally affordable by the shipping industry, who in any case would not receive the resulting security benefits and have little incentive to act. A lower cost, effective solution could lead to the development of a substantial market, but it would require strong government intervention to bring this about.

3.11 Threat Detection based on Data Fusion and Domain-Specific Threat Analysis

What is it?

A consequence of increasing automated detection monitoring from digital sources of information (for example from sensor networks or CCTV data) is that this will lead to increased vigilance in respect of raising alerts that need to be responded to. Since terrorist or criminal activity tends to occur at low frequency relative to benign incidents that result in monitoring data with a similar profile, this creates some specific challenges.

If a system cannot effectively distinguish between genuine threats and benign incidents this creates increased probabilities of failure to detect real threats. Since there is a cost to responding to and resolving any detection event, this can be exploited by attackers who will use false positives to masquerade a genuine attack. Threat detection systems based on the integration and analysis of data from a range of security sensor networks, combined with domain-specific threat modelling and analysis, should enable the discrimination of genuine threat indicators (for example border security or passenger screening system alerts) from behaviours which are benign.

Such systems will improve discrimination in Homeland Security systems between false positives and genuine threats, based on increased leverage of multiple factors including:

- exploitation of multiple sources of event data – data fusion
- innovation and combination of new algorithms – algorithm fusion
- increased use of domain specific threat modelling – deep threat modelling.

In theory, the availability of better quality data in greater volumes should dramatically improve the capabilities to successfully resolve boundary incidents that can lead to detection failures. In practice the availability of extra data can exacerbate the problem with an increasing number of detection incidents to resolve.

The problem is widespread and pervasive through all security systems but sensitivities within Homeland Security are particularly acute due to the issues of scale (for example in border monitoring), and the potentially high cost of a failure to detect. It is possible of course that this is inherently an insoluble problem, and that there is always a profile boundary between threats and benign alarms that will forever intersect.

What application does it enable?

The problem of reliable discrimination between false positives, genuine threats, and attacker stimulated events pervades all aspects of intelligence surveillance relating to detection of threats or intrusions. These include primarily:

- digital surveillance systems for local networks and facilities
- physical surveillance systems for perimeter security to protect critical infrastructure and public places
- data analysis and intelligence analytic systems that aggregate data from lower level surveillance systems and combine this with other information.

The vision – A coordinated digital security and surveillance system that exploits sensor and monitoring information from multiple and diverse sources including digital networks and systems, application logs, and alert information that derives from physical sensors or CCTV analytic software. The evolution of algorithms should eventually be able to exploit the increased availability of information to significantly increase the reliability of threat detection, without the overhead of false rejects.

The reality – In recent years the effective performance of Intrusion Detection Systems has radically improved, with that improvement attributable to a number of factors including:

- supplementing network based sensors with host/application sensors
- supplementing signature-based monitoring with behaviour-based monitoring that searches for anomalies
- exploitation of vulnerability assessment to discount detected potential attack behaviours that can have no adverse consequences.

Digital intrusion detection systems can now be supplemented with Security Event Correlation (SEC) systems that can analyse information from a wider set of information sources and can explore behavioural indicators of low lying threats based on analysis windows that are of arbitrary duration.

Physical intrusion detection systems based on sensors, as applied for example to physical security, currently tend to work as independent alert monitors. The opportunities for improvement of physical intrusion detection systems, based on data fusion and SEC style technologies, are currently under-exploited in the field.

The next step – It is most likely to be the case that the key to improvement of anomaly detection in large databases is to establish an algorithmic approach where large volumes of data from differing sources are turned to the advantage of the system. Whilst multi-variable analysis creates the potential for more information the exploitation of multiple scoring factors is inherently difficult, especially in simplistic scoring algorithms based on weighting factors and alert thresholds.

However, large volumes of data also potentially lead to much better statistical profiling of what constitutes normal behaviour. The form of profiling may be further enriched based on exploitation of domain modelling that is specific to certain sub-spaces of variable, population or value ranges. Consequently, a combination of heuristic and quantitative characterisation of combinatorial profiles across different variables may yield more robust means of identifying anomalies.

Market and ecosystem

Technologies that exploit intrusion detection algorithms are a well established sector within digital security products and are increasingly referred to as Intrusion Protection Systems, in acknowledgement of the fact that they can be configured to automatically react to close off the threat from an identified threat or attack. There is a well established market for provision of security products. The current products are still going through a phase of high innovation in which new analysis tools are incorporated within existing products. There are options for a technology provider to license specific components to existing players instead of creating an alternative product.

By contrast, the market for surveillance systems based on data fusion across standard sensors such as those that are used in perimeter security is much less mature. Providers of SEC technologies already target these applications by offering to provide a configurable threat analysis engine that can provide comprehensive threat assessment across an arbitrary set of inputs. However the adoption of such technologies seems to be immature, and whilst the need for data fusion seems to be universally recognised, there is little evidence of awareness of the potential for technology cross over from the digital security domain.

However, the characteristics of intrusion detection in the digital security domain have been the subject of many years' research, and a market for this already exists independently of Homeland Security. It is much more likely that it is within different domains of application that are most likely to yield opportunities for novel approaches. For this category of application it is most likely to be addressing government security markets that are specific to the management of intelligence.

What are the unmet needs?

- High performance models for discrimination of anomalies that are indicative of genuine threat from behaviours that are merely unusual
- Effective management of multi-variable analysis across large data-sets of disparate data-types
- More effective exploitation of domain-specific models that enable more effective characterisation of anomalies that are most likely to be indicative of a threat

Market size

Market size is estimated to be of the order of USD1.5 billion per year based on projections of market size for digital security intrusion detection/prevention systems.

Market barriers and enablers

- Drivers and Enablers
  - High level of awareness of the need to exploit data fusion more effectively
  - High cost of addressing false positives
  - The tendency of high frequency false positives to mask genuine threats, and render the security mechanism ineffective
  - Well established market exists – and this provides incremental value within existing infrastructure and processes
- Barriers
  - Difficult to develop, test and prove a new technology without access to some meaningful test data. This hugely favours current players or trusted government suppliers
  - This is an inherently hard problem and lots of clever people have already addressed it.

Timescale (market window)

The market opportunity is likely to be in a 3 to 5 year time frame, based on the historic pace of adoption of technologies within the security market.

Key players

Players in this market include companies addressing the opportunity from different viewpoints, including data fusion, internet security, network intrusion detection/prevention and intelligence analytics technology.

- Surveillance data fusion
  - Raytheon Systems Limited: http://www.raytheon.co.uk/products/isr.html - Major player in the intelligence and security sectors
  - Virage: http://www.virage.com - Intelligent video analytics
- Tier 1 Intrusion detection/prevention companies
  - Internet Security Systems: http://www.iss.net – Prevention of internet based threats
  - CISCO: www.cisco.com/ – Major player in network security
- Tier 2 Intrusion detection/prevention companies
  - TippingPoint: www.tippingpoint.com/ - Intrusion protection
  - CheckPoint: www.checkpoint.com/ - Intrusion protection
  - SourceFire: www.sourcefire.com/ - Intrusion protection
  - TripWire: www.tripwire.com/ - IT configuration audit and control
- Technology specialists
  - ArcSight: http://www.arcsight.com/ - Provision of security and compliance intelligence by identifying, prioritizing and responding to security threats and network changes
  - Memex: http://www.memex.co.uk/ - Intelligence management software solutions

Conclusion

Detection of genuine threats based on data fusion, effective analysis and (security) domain-specific threat modelling is likely to form a key component of many Homeland Security systems in the medium term, based on effective discrimination of genuine threat indicators from behaviours and sensor data that are benign. This will require substantial performance improvements in (for example) methods for reliably identifying anomalies from multiple sources of event (sensor) data and assessing anomalies against threat models. Such systems could command a substantial market.

3.12 Vulnerability Assessment

What is it?

Vulnerability assessment consists of a software service that supports self assessment of vulnerabilities and evaluation of alternative mitigation strategies. The tool would incorporate an extendable WIKI of threat analysis domains and associated best practice solutions, where the core content is moderated through authorised contributors and experts.

What application does it enable?

Primarily addresses the private sector Homeland Security market which is expected to finance its own vulnerability assessments and security compliance policies, without access to the level of funding that has been allocated for other security infrastructure such as airports.

However the broader application for a vulnerability assessment and security policy management tool should extend more generally to the wider commercial sector that has a need for cost effective security risk management, but has limited access to security expertise.

The vision – A software based expert assistant that can help current organisations assess and address their specific security requirements, without the need to draw on high cost security expertise that is in short supply. In reality, Security Threat modelling and the construction of policies is heavily pattern-based both in terms of characterisation of the vulnerability itself, and the risk/benefit/cost basis for identifying an effective course of action. The characteristics of wide-spread adoption of good security practice, that affordably exploits and informs best practice, are well suited to the provision of vulnerability assessment tools.

The reality – Niche products already exist that address specific problems. For example the Transport Security Administration (TSA) in the US has been developing tools since 2005 that support local transportation providers in the assessment of vulnerabilities to support formulation of security plans.

In the wider market, companies such as Relational Security provide an open and adaptable framework for risk and compliance assessment, which they refer to as RSAM (RSAM does not have a formally defined acronym, but can be interpreted as Security Risk Assessment, Management, Policy and Compliance). This has templates for standard regulation such as PCI Data Security Standard (Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability and Accountability Act) but also enables people to create their own templates. The RSAM tools are based on questionnaires and more broadly on Health and Safety principals of identifying risks and controls as a means to defining policy.

The next step – Any number of niche products that are specific to a single domain would continue as non disruptive offerings that address specific verticals. The next step for a break-through product is one which enables the separation of security knowledge domain from the core application that performs vulnerability threat assessment and security policy formulation. Note that RSAM tools do this to a degree, albeit at a shallow level.

This product addresses multiple markets simultaneously and whilst the fundamental principals of threat analysis, security policy formulation and cost-benefit assessment of best practice solutions would be universal, domain specific models can be developed and enhanced separately from the software.

Market and ecosystem

This could be provided to the market and sold via government agencies who seek to instil best practice through empowerment and self-help, such as already demonstrated by the TSA.

Whilst the role of the product is to reduce the reliance on external security consultants it is also believed that the tool would be exploited by the security consultancy industry as a means of establishing market presence, by enabling efficient execution of a security audit which achieves a high level of engagement from the business user. However no such current market exists and there is no strong evidence of a market beyond the strong positive response that was received in the primary research workshops.

What are the unmet needs?

- A cost effective visualisation tool to assist in vulnerability assessments and subsequent formulation of security policy
- A means of formally assessing risk based on combined threat modelling and cost benefit assessment
- Access to solution patterns of best practice that make security policy formulation more accessible to non-security professionals

Market size

This opportunity is essentially that of a new software service. This has not been covered by analyst estimates of market size, but based on experience in these markets we expect market size to be less than USD10 million per annum (source: ITI Techmedia estimate).

Market barriers and enablers

- Drivers and Enablers
  - Easy to distribute and use
  - Can be offered on a trial basis as an internet based service
  - Supports value added reselling through security consultancies who can customise the domain characterisation and security policies to align with specific domain expertise

- Barriers
  - The user may be unlikely to be the buyer
  - If the TSA policy is followed more widely then it is expected the tool would be sold to a government agency and then distributed to operational members without payment from the ultimate user
  - It is not clear that users would perceive significant value over and above that which is offered by RSAM tools.

Timescale (market window)

Based on feedback from government advisors, we expect a market for vulnerability assessment products to develop in the next 3 to 5 years.

Key players

There is no current commercial activity in this sector of which we are aware.

- Software tools provider for standard risk assessments: http://www.riskworld.com/SOFTWARE/SW5SW001.HTM
- Relational Security – develop security risk assessment tools that address self-help for security compliance such as PCI or HIPAA: http://www.relsec.com

Conclusion

A product opportunity exists for a cost effective visualisation tool to assist in vulnerability assessments and subsequent formulation of security policy, across many vertical market areas. Whilst in Homeland Security terms the likely market for such a system is relatively small, this opportunity could form the basis for the growth of a significant company.

3.13 Information Intelligence – Privacy and Security Controls

What is it?

It is abundantly clear that the nature of global intelligence monitoring systems that extend investigative search beyond guilt by association models to analysis and monitoring of the wider population raise significant issues relating to data protection. The acquisition, transmission, analysis and dissemination of subsequent intelligence are sufficiently contentious to inhibit the development of such systems, if not prevent them entirely. This is evident in the lowering of ambitions of Total Information Awareness which was subsequently downgraded to a classified research project.

The extent of reach of any such system, and the large number of potential recipients of intelligence, has implications both for security of that intelligence and protection of the system against abuse. Authorisation controls and credentials provisioning need to be provided on a large scale and extensive innovation is required to remove both the actual and perceived level of privacy invasion. It is known for example that to be effective such systems may require enablement of data correlations that reveal information that is by definition personal. They may also require access to data such as GPS positional information that is intrinsically personal in nature.

The level of resistance to such systems should not be understated nor should the technical challenge be under-estimated. There is an inherent conflict between privacy protection and global surveillance systems that may be a contradiction that cannot be overcome. However it is clear that effective resolution of that conflict would be a critical enabler for global intelligence systems.

What application does it enable?

Within the context of Homeland Security markets the provision of scalable, strong security will enable the following applications:

- scalable distributed processes for credentials provisioning, including issuance of passports, identity cards and drivers' licenses
- issuance of digital authorisation credentials for trusted administrators, and all personnel who have access to protected intelligence and personal information
- provable privacy protection of benign data that does not lead to discovery of intelligence.

The vision – A global intelligence system that uses a combination of data minimization, data isolation and strong access controls that guarantee auditable protection of security intelligence and enforces secure channels for transmission and authentication of end points for dissemination of discovered intelligence. It is not possible to be prescriptive of the kinds of technology that would enable such systems to be built. But the following may be possible aspects:

- the security model provably enforces absolute secrecy of benign data that does not lead to discovery of significant intelligence
- analysis engines operate exclusively on data that was provably minimised to the extent that related personal identity could not be discovered from that information
- analysis engines execute exclusively within processing environments that are provably protected against subversion or interception of data – e.g. tamper proof hardware security modules or processing environments
- the promotion of intelligence from minimized domain to the actual domain that reveals associated person(s) should be subject to strong controls that guarantee authenticated access and tamper proof audit trails
- the processes for registration of the identity and access control rights of authorised users are subject to strong controls that guarantee integrity through authentication and audit controls
- the provision of guaranteed audit trails that monitor all privileged access and can be attached to an independent audit function of a trusted third party watchdog.

It should be noted that the mechanisms for provisioning of identity and access controls have broad application throughout all Homeland Security applications.

The reality – Current reality for global intelligence is R&D systems like Tangram which rely on public assurances in respect of the extent of contained data, and the nature of operations that are being applied. Within the UK and Europe such systems are unlikely even to be commissioned unless the larger scale security and privacy problems are addressed. Current reality for identity management and access controls is that these are increasingly being subject to standards such as SAML that should address scalability at the broad level of systems integration. There remains however a level of disconnect between identity registration processes and the underlying technology which at its strongest relies on PKI solutions.

The next step – In the absence of scalable, trusted systems to ensure information privacy there is significant uncertainty as to when significant government procurements for security controls which enable pervasive intelligence will occur. However assuming that the threat from terrorism and the desire for privacy are continuing trends, solutions in this area are likely to start to be developed within the established vendor/government ecosystem in the near term.

Market and ecosystem

The development of security infrastructure is increasingly being viewed as something that is pervasive throughout enterprise IT architectures rather than as an additional layer that is separately procured and added. A significant channel to the wider security market is through Systems Integrators and prime contractors who deliver large scale IT systems.

Within Homeland Security the engagement is directly with the Passport Services in terms of the management of their provisioning services which in many places, including the UK, are being subject to a major security overhaul that requires much more robust processes surrounding registration. This is increasing demand for a more distributed provisioning process which will be

met through bespoke systems development. Specialist providers of integrated security services are likely to be the most relevant players in this market.

The ecosystem for the provision of technologies that enable the development of a global intelligence surveillance and monitoring service has been discussed in previous sections.

What are the unmet needs?

- Scalable provisioning of high security identity registration services and access control
- Verifiable protection of privacy within large distributed or federated database systems
- Strong auditing technology that guarantees integrity of the system in respect of potential abuse

Market size

The market size within Homeland Security is too early stage to quantify. There are also significant question marks over whether or not the level of security within government systems will ever extend beyond good practice, since security tends to be a single consideration within a much larger system procurement. The wider market for high security services that are scalable, affordable and easy to integrate is huge – analysts expect markets for security applications and identity management to reach ca. USD9 billion per annum by 2008 (source: Gartner, Radicati).

Market barriers and enablers

- Drivers and Enablers
  - Need for governments and law enforcement agencies to exploit available data in ways that are compatible with wider concerns
  - Need to manage provisioning of high security authentication and access control across larger networks of participants
  - Increasing activity in the general market to introduce scalable, affordable security infrastructure that supports identity management in response to increasing regulatory compliance
  - Growth in service oriented architectures, which open up access to enterprise systems across multiple organisations, or component businesses in a post-merger corporate
- Barriers
  - Security is increasingly seen as an aspect of wider systems. The channels to market for new entrants with disruptive technologies are unclear
  - There is significant uncertainty relating to when and if significant Government procurements will occur that will leverage the kind of security controls that enable pervasive intelligence systems

Timescale (market window)

The projection for growth of disruptive technology to address this market is based on comments from primary research, which confirmed the insufficiency of current technologies to effectively address the scale of the requirement. It is likely however that for the next 5 years, deployment will be based on incremental change to current security provisioning and the growth of open standards for enterprise security middleware. The history of the security market shows that the pace of adoption is slower than the assessed need would imply, and this is clearly illustrated by the tortuously slow adoption of PKI. Whilst the long term market pressure is undeniable, the opportunity for mass market technologies will take about 5 years.

Mature assessment of security markets clearly shows that market penetration only occurs in response to regulatory obligations, an inescapable market pressure or else a drastic reduction in cost and pain of adoption. For the mass market, which is not compelled by regulations or security sensitive customer base, it will require huge simplification in the delivery of security technology and provisioning of associated certification processes before accelerated adoption will occur. It is possible that the Homeland Security applications may lead the market for technologies such as federated identity and single sign on, partly in relation to enabling

concepts such as Total information Awareness to operate within the bounds of political acceptability. It is however difficult to see this moving more quickly than the broader market.

Key players

Leading players in this market include:

- Carnegie Mellon Data Privacy lab.: http://privacy.cs.cmu.edu/index.html
- Liberty Alliance project – for protection of privacy: http://www.projectliberty.org/
- RSA Security: http://www.rsa.com/ - Information-centric approach to security
- Verisign Inc: http://www.verisign.com/ - Leading provider of PKI and certificate services:

Conclusion

The development of security systems which ensure the protection of personal information would remove a significant barrier to the adoption of pervasive national monitoring systems to detect threats and identify suspicious behaviour. The development of an effective system is likely to be technically challenging, and the size of this emerging market is uncertain. However the importance of systems which perform the required combination of security and privacy functions is likely to grow, and this could be the starting point for a very significant market space.

3.14 Market Opportunities not Prioritised

The following table lists the areas which were assessed but were not viewed to offer the greatest opportunity. The key reason for not progressing these areas is outlined.

Opportunity	*Summary*	*Key reason for not prioritising*
Biological agent detection	Detection systems for biological agents at airports, border crossings and critical infrastructure sites	Very difficult detection problem – unlikely to be successfully addressed in the short-medium term
Biometrics database	Creation and use of a centralised biometric database, e.g. for passport validation	Political factors strong constraint on implementation; timescales likely to be lengthy
Biometrics: Iris recognition	Applications based on authentication of individuals using iris recognition	Mature, well-understood technology. Cost and usability constraints likely to mean slow adoption
Chemical agent detection	Detection systems for chemical agents at airports, border crossings and critical infrastructure sites	Small, mainly military market. Limited scope compared to explosives detection
Coastline monitoring systems	Use of imaging systems for marine detection and surveillance	No large scale systems deployed. Little government appetite for the huge task of monitoring coastlines
Drinking water security	Monitoring and protection of the drinking water supply	Little activity likely in this area in the absence of a “kick-start” incident. Low-tech monitoring approaches preferred.
Ground sensors	Self-powered, self-networking sensors for deployment in remote	Small, mainly military market. Spin-offs to civil markets possible, but timescales likely to

Opportunity	*Summary*	*Key reason for not prioritising*
	land border regions	be long
IED countermeasures	Detection and deactivation of Improvised Explosive Devices	An area of strong current interest, however many solution areas are military (e.g. communications jamming). Surveillance aspects are covered by areas selected as high priority (video analytics, CCTV)
Interoperable communications	Interoperable communications systems for first responders to emergencies	Problem largely addressable by current radio technologies and political will (spectrum allocation and funding)
Nanotechnology sensors	Nanoscale sensors (e.g. sensor on chip) for detection of chemical, biological and other agents	Interesting area, potentially highly significant but commercialisation timescales likely to be long
Nuclear material detection	Detection of (shielded) nuclear material at ports and border crossings	Largely addressable by engineering and design rather than by breakthrough concepts
Passport issuance/validation	Effective solutions for passports, including enrolment, issuance and authentication	Operationally and politically difficult, hence timescales likely to be lengthy.
RFID tracking	Use of RFID for tracking individuals or objects for security purposes	Limited potential for use of basic RFID in Homeland Security
Smart identity cards	Use of ID cards to provide identity for security applications	Significant bottleneck due to privacy concerns and little traction for the use of ID cards in commercial services
Underwater port security	Underwater detection systems to protect ports from external threats	Little government interest in civil applications; potential military targets already protected
Unmanned aerial vehicles	Micro-scale UAVs for security and surveillance applications	Interesting area but regulation is currently a show-stopper. This is unlikely to change quickly
Voice verification	Recognition of individuals through their vocal tract characteristics	Small market likely for application in Homeland Security
Workflow and co-ordination (emergency response)	Systems for co-ordinating emergency services responding to large scale emergencies	Opportunities likely to involve process improvement and workflow, hence limited IP opportunity
X-ray imaging	Use of X-ray imaging for object detection and materials analysis	Security applications relatively mature

Figure 8: Non-prioritised market opportunities [Source: ITI Techmedia]

4 CONCLUSIONS AND NEXT STEPS

This section includes a short conclusion to the report together with the next steps that ITI Techmedia will take to investigate opportunities arising from the Homeland Security foresighting activity

4.1 Conclusions

This report has outlined the Homeland Security market with a focus on the European market requirements. An application driven segmentation was used to frame the market opportunities and to identify common requirements across multiple segments. The market potential is clearly extremely significant with market spend in 2007 around USD27b which is expected to grow to USD 90b by 2017. However, this is a complex market where the governments are the main customer and the need to respond to individual incidents (or the threat of such incidents) drives spending. However, given these conditions, governments may not invest in the most important areas to defend against in the future.

Despite the scale of national Homeland Security contracts, a range of players exist in the ecosystem. Major players, such as large defence contractors work alongside smaller, technology-based companies to carry out funded R&D.

It is clear that, despite significant spend over the last 5 years, there are still some unmet needs, many of which have very demanding and interesting technical challenges which offer opportunities for innovation. From these, 11 top opportunities were identified and validated using a combination of secondary and primary research:

- Airport perimeter security
- Biometrics: Face recognition
- Border monitoring and control
- CCTV – Intelligent CCTV systems
- Data analysis and threat detection via intelligent data mining
- Effective threat detection based on data fusion and domain-specific threat modelling & analysis
- Explosives detection
- Freight container security, monitoring and tracking
- Information intelligence, privacy and security controls
- Video analytics
- Vulnerability assessment

They span broad segments of airports, land borders, seaports, infrastructure protection, emergency response and information security. A number of these areas offer extensions to the commercial environment which would help reduce the reliance on government commitments.

4.2 Next Steps

ITI Techmedia has reviewed the identified opportunities to assess which are the more promising area(s) to investigate further. In particular, the following criteria were considered:

- the competitive advantage delivered by meeting the unmet needs of the opportunity, i.e. assessing whether the market opportunity is credible and durable
- the key components (functional needs) which should be encompassed by a successful solution
- the potential for creating new IP
- Scottish skills base in relevant technologies
- key risks

Following this analysis four areas have been prioritised by ITI Techmedia for further study and engagement with the Membership. These are:

- CCTV and video analytics
- explosives detection
- border monitoring
- effective threat detection

ITI Techmedia welcomes R&D Programme proposals or expressions of interest in these areas to understand the capabilities and commercial interest within Scotland. ITI Techmedia also intends to organise a briefing to present these opportunities in more detail. If you are interested in receiving further information on this or how to make a proposal, please contact Mairi Robertson, Market Analyst, ITI Techmedia (mairi.robertson@ititechmedia.com).

5 APPENDIX 1: GLOSSARY OF TERMS

CCTV	Closed-circuit television
CT	Computed Tomography
DHS	Department of Homeland Security (US)
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
HOSDB	Home Office Scientific Development Branch
HSARPA	Homeland Security Advanced Research Project Agency (US)
ID	Identity
IP	Intellectual Property
IR	Infra-Red
ISACS	Information Sharing and Analysis Centres (US)
ITT	Invitation To Tender
PCI	Payment Card Industry
PKI	Public key infrastructure
RFID	Radio-frequency identification
RSAM	RSAM does not have a formally defined acronym, but can be interpreted as Security Risk Assessment, Management, Policy and Compliance
SAML	Security Assertion Markup Language
SEC	Security Event Correlation
SME	Small or Medium sized Enterprise
TIA	Total Information Awareness
TSA	Transport Security Association (US)
UAV	Unmanned Aerial Vehicle
WIKI	Collaborative technology for organising information on Web sites