Market Trends in Homeland Security Technologies

Bahar Barami
Senior Economist, DTS-24
Volpe Center
617-494-2150
Barami@volpe.dot.gov

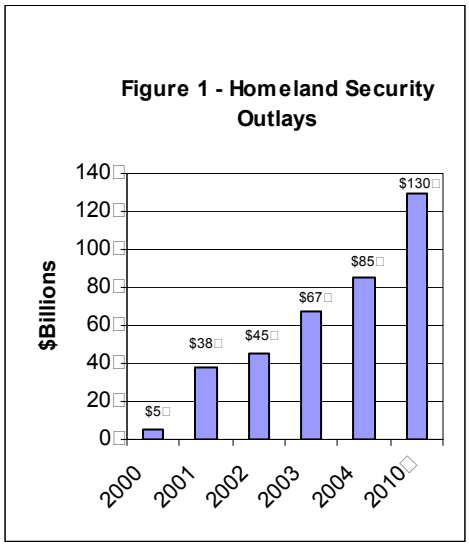
Paper presented at the:

IEEE Conference on Technologies for Homeland Security
Held at the Volpe Center
Cambridge, MA, April 21-22, 2004

This paper reviews the dimensions of the homeland security (HS) technology markets, identifies their application areas and the risks they are designed to mitigate, and asks: How well have these technologies performed – in the marketplace and in the field – and how are emerging technologies in robotics, nanotechnology, and biotechnology likely to transform these markets in the near future?

Size of the Markets

No reliable figures are available for the total public and private expenditures on HS technologies. One source estimates the total HS outlays – by federal, state, local, and private entities – to have grown from $5 billion in 2000 to $85 billion in 2004, and forecasts that they will grow to $130 billion by 2010 – and possibly as high as $210 billion (HSRC, 2003, See Figure 1.) By another estimate, the current public and private security outlays are roughly $72 billion (*Federal Reserve Bank of New York,* 2002.) Yet another study estimates the 2003 public and private sector security expenditures at $100 billion (Richard Miller & Associates*,* 2003.)



The wide range of estimates on the size of security markets suggests that, to discern any meaningful trends, we need to know who makes the expenditures and for what purpose. We know that the 2004 DHS budget request was for $41.3 billion. By adding the security outlays of all 32 federal agencies, the total federal budget request for 2004 rises to $52.7 billion, as reported by a recent OMB document.

Outlays of the private sector are harder to account for. By one estimate, the annual private sector security costs could range between $18.5 billion to $41 billion (Navarro and Spencer, 2001.) Another report, a pre-9/11 study conducted for the National Institute of Justice, estimated the total private security expenditures at $100 billion (Cunningham, 2002.) Given that more than two thirds of the total U.S. infrastructure is owned by the private sector, the high-end estimates for the private sector security outlays are not too farfetched. However, given the dual-use nature of many security technologies, it is important to be able to identify the security market segments accurately and have a more precise estimate of the private sector share. The following sections demonstrate the difficulty of identifying the sub-sectors within these markets.

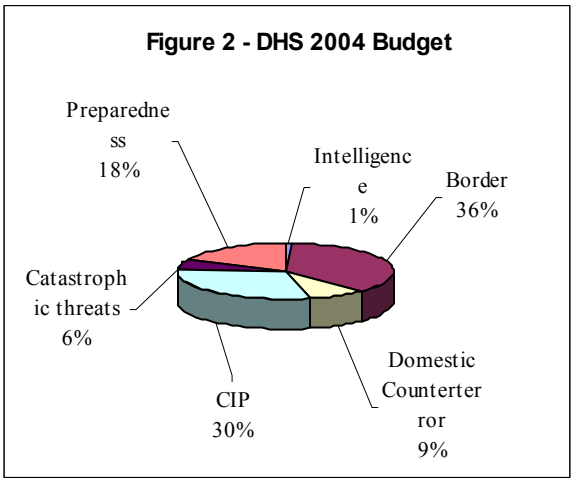
Application Areas

What risks are these expenditures supposed to protect against? In defining security markets, how do we distinguish between expenditures made exclusively for security purposes and those with tangential security benefits? An overly simplified example is the security uses of the "duct tape." The annual civilian and military market for the duct tape is $100 million. Demand for this product – a longtime military staple used for equipment repair and ammunition packaging – skyrocketed in 2003 subsequent to a series of DHS recommendations for civilian safeguards during periods of elevated terror alerts. Are duct tape sales included in estimates of the size of security markets? The point here is that we don't quite know what is included in the statistics on the size of the HS markets.

To identify today's HS markets more accurately, we can create a risk-based framework with four

risk-mitigation objectives: 1) Prevent unauthorized entry; 2) Detect treat; 3) Protect critical infrastructure; and 4) Prepare, respond and recover. Figure 2 shows the distribution of the 2004 DHS budget, with the largest share, $15 billion, allocated for border security, followed by $12 for critical infrastructure protection, and $7.4 billion for emergency preparedness.

Figure 2 - DHS 2004 Budget



The first application area – Prevent Unauthorized Access – is for people and passenger screening at borders/ports-of-entry, at workplace entrances, and at points of access for cyber systems. This application area deploys a wide range of technologies based on radio-frequency identification (RFID,) smart cards, and biometrics for identification, authentication, and authorization. The size of the market for devices to screen people is estimated to have grown from $590 million in 2001 to $800 million in 2003. By 2010, the U.S. markets are expected to grow to $1.85 billion (HSRC, 2003.)

Application of biometrics for access control is relatively new. This technology has become a growing market since the events of September 11, 2001. By one estimate, the biometrics market is expected to grow fourfold by 2007 from the present $1 billion. By another estimate, this market in 2000 was about $395 million, and is expected to grow as high as $1.9 billions by 2005 (Traeger, 2002.) As alternative modes of authentication – fingerprint, iris scan, retinal scan, facial recognition, gait recognition, voice verification, etc. – are field tested, market shares are likely to reflect a loss in some products and gains in others. Growth in enabling technologies – e.g., new products introduced for voice scanning and facial recognition – is also likely to compound the surge in demand for biometric devices.

The second risk category – Detect Threats – involves applications for cargo and vehicle screening, detection and surveillance systems, with technologies such as video monitors, explosive detectors, sensors, X-ray machines, and computerized data analytic capabilities. Container security outlays for maritime security has grown from $60 million in 2001 (when outlays were spent primarily on drug interdiction) to $750 million today, and expected to grow to $1.4 billion by 2010 (HSRC, 2003.) In addition to the rising federal demand for airport and seaport security, markets for private applications are also growing. Workplace surveillance, for instance, has become a growing security market. Sales of surveillance technologies and biometrics devices have risen steadily. An estimated 80% of the major U.S. companies electronically monitor their employees in some form, according to a survey by the American Management Association: 38% conduct video surveillance, 47% monitor e-mail, 36% monitor computer files, and 43% monitor phone usage (Farmer and Mann, 2003.)

The third risk category – Protect Critical Infrastructure (CIP) – involves applications of sensor technologies and protective devices to reduce vulnerabilities and harden the infrastructure. The OMB budget request for 2004 was for $12.2 billion to cover infrastructure protection efforts of 32 federal agencies. Private expenditures on workplace security are estimated to have generated recurring costs of about $18 billion per year – including, ID checkpoints, guards, gates, entrance barricades, etc. For cyber security – another CIP risk mitigation area – private outlays have been estimated at proximately $15 billion per year (Bernasek, 2002.)

For the fourth risk category – Prepare-Respond-Recover – location and communications systems routinely rely on wireless, cellular and satellite

technologies for tracking and location-identification functions to support emergency response and domain awareness. Many of the technologies in this category are dual-use, with a wide array of civilian applications. Cellular and digital telecommunication, for instance, is a large component of the commercial technology market unrelated to security. Similarly, GPS navigation devices for locating and tracking assets comprise a $16 billion market, but the precise breakdown of the military and civilian market segments for GPS is not fully known. (*Business Week*, 2003.)

The dual-use nature of many security products could initially lead to inflated estimates of the size of security markets, but in the long run it is likely to generate secondary security benefits and bolster the rate of market penetration for new technologies. Another factor that can indirectly benefit market growth for security technologies is that in recent years the direction of the flow of dual-use technologies between the military and civilian sectors has been reversed. In the 1990s, strategies for cutting defense spending led to concerted efforts to cut procurement and supply costs by using commercial off-the-shelf (COTS) products for military use. Today, the trend is in the opposite direction. According to the manager of the Montana State University TechLink Center in charge of facilitating technology exchanges between the DOD and the private sector, competitive pressures on private companies to cut costs have led to a major shift in the private sector attitude towards military technologies. Many firms have concluded that adopting devices developed by the military can be cheaper than developing them in house, a shift in part driven by the fact that the products have already passed many demanding performance tests (*Business Week*, 2003.)

Market Performance

Evaluating how well a technology does in the market is closely coupled with the process of evaluating its technical performance. The technical performance of a device – e.g., device failure rate or false positives – is continually investigated and fully reflected in its market capitalization. Several factors directly or indirectly influence the direction and growth path of a technology: a drop in production costs/product prices, emergence of product substitutes, and entry of new technologies.

Plummeting costs have been a major factor in market growth for many HS products. RFID tag prices, for instance, have dropped from $5 to $10 several years ago to $1 today, and are expected to drop as low as $0.50 or $0.10. In biometrics, the products were first used for security of computer networks, and available only at a high price. Increasingly, the prices of biometric devices are declining as new markets develop. Introduction of inexpensive standardized components such as DSPs (digital signal processors) used with many biometric devices has also helped with the rise in market penetration.

Entry of new product substitutes has also changed the composition of the markets. For instance, barcode products– with a market size of about $6.5 billion – are rapidly being replaced by the more versatile RFID products. RFID markets – comprised of companies that design and manufacture data transponders and radio frequency readers – are currently about $1 billion, and are expected to grow annually at about 20% to reach about $4 billion by 2008. Security applications of RFID are relatively new. Until recently, RFID products were used almost exclusively for tagging equipment for asset identification and inventory control. With the growing use of RFID tags in surveillance devices, growth in this market is likely to be even more rapid since most market forecasts for RFID products have not included growing security applications. Development of new applications for RFID tags – e.g., uses by firms such as WalMart for supply-chain tracking, or for uses in baggage handling and employee ID and access control – have further helped expand the markets. Also galvanizing the markets for RFID has been the growth in dual-use products created by the fusion of RFID tags with sensors for detecting and measuring motion, carbon emissions, or other airborne contaminants for industrial, medical and municipal uses. Sensor fusion has led to growth in another market

specializing in household applications for monitoring the movements of elderly citizens (*Technology Review,* 2003.)

Emerging New Markets

Developments in robotics, nanotechnology and biotechnology are likely to significantly impact security markets. Advances in nanotechnology, for instance, have led to growth in new security devices based on the fusion of miniature RFID transponders with biochemical sensors. Because of their small size and versatile detection capability, these sensors can be used pervasively and inconspicuously to provide a blanket of protection. Another security application of biotechnology is in products being developed based on research in terahertz radiation (T-ray), which is likely to lead to the replacement of X-ray machines with T-ray imaging devices that detect an object's chemical composition.

Robotics is another emerging application area likely to transform security markets. A robot can effectively replace human operators by automating or augmenting the human tasks which are "dangerous, difficult, dull, or demeaning," as described by the director of the General Robotics, Automation, Sensing and Perception Lab at the University of Pennsylvania (*Robotics Trends*, 2003.) The size of the civilian – with industrial as well as household uses – and military markets for "bots" is growing, with some 778 million units sold last year. In 2003, according to the Robotic Industries Association (RIA), the robotics market was a $10 billion industry worldwide, with $3 billion in U.S. (*Robotics Trends*, 2003.)

Robotics entered a new market phase with the events of 9/11 and the U.S. military operations in Afghanistan and Iraq. Prototype remote-controlled robotic devices were hastily assembled to conduct search and rescue operations in the wreckage of the World Trade Center. More recently, robotics entered mass-production when the military began deploying robots overseas for combat operations, using PackBot, a robotic device manufactured by iRobot. PackBot is a 42-pound, rubber-treaded crawler equipped with wide angle zoom cameras, sensors, and Pentium 3 processor brains connected to an Ethernet hub, capable of relaying intelligence to the local command center. During the search for WMD in Iraq, the radio-controlled PackBot, equipped with chemical-agent detectors, was dispatched to search areas to navigate with the help of GPS technology and digital compasses, and transmit radio signals back to the command center. PackBot is also being tested by several cities and police departments for use in search and rescue and hostage situations (*Business Week*, 2003, *Robotics Trends,* September 6, 2003.]

Another robotic device with security application is the next-generation Small Unmanned Ground Vehicle (SUGV), developed for the Army by iRobot as part of the Army's Future Combat Systems (*Robotics Trends,* 2003.) At Carnegie Mellon University, also, scientists are working on robots for DOD that can drive trucks in convoys, steering a vehicle without human help from Los Angeles to Las Vegas.

Portable unmanned aerial vehicles (UAVs) — remote–controlled drones the size of a model airplane – are another security device likely to emerge as a major commercial market. These UAVs are essentially aerial robots that are able to carry missions autonomously without human command or intervention. Increasingly, they are capable of flying longer missions, carrying more sensors, and collecting more data. While regular size UAVs have been around for decades, the portable ones – small enough to fit into a briefcase and snapped together in five minutes – are the products of the recent Iraq war. They cost between $50,000-$100,000, compared to millions of dollar for a regular size UAV. Each portable UAV has a battery that lasts an hour, can survive up to 100 landings before needing to be refurbished, and can carry cameras and chemical agent detectors. Because of their small size, they can readily be used for surveillance functions, as they are less conspicuous than a pilot-navigated surveillance plane or larger UAVs – which can be shot down with small arms. The market size for portable UAVs is currently estimated at tens of millions of dollars, but is expected to grow to several hundred million dollars. [*Business Week,* April 2003.)

To sum up, we are witnessing a major leap forward in security applications of advanced technologies. Though many are early in the product life-cycle or at the prototype phase, the development times are shrinking and new products are entering the market rapidly. Homeland security markets are thus likely to be radically transformed by new developments in biotechnology, nanotechnology, robotics and breakthroughs enabled by the fusion of several basic technologies.

References

Bernasek, Anna, February 18, 2002. "The Friction Economy," *Fortune Magazine*.

Business Week, April 9, 2003, "War, Technology's Proving Ground," http://www.BusinessWeek Online.com

Cunningham, William C., 2002, "U.S. Private Security Trends," *Hallcrest Systems, Inc*.

Farmer, Dan and Charles Mann, April 2003. "Surveillance Nation," *Technology Review*.

Federal Reserve Bank of New York, 2002. "What Will Homeland Security Cost?" *Economic Policy Review.*

Homeland Security Research Corporation (HSRC), 2003. "Homeland Security Industry – Trends." www.hsrc.biz

Navarro, Peter and A. Spencer, 2001. "Assessing the Costs of Terrorism," *The Milken Institute Review.*

Office of Management and Budget (OMB), 2003. "Combating Terrorism," A Report to Congress.

Richard Miller & Associates, July 1, 2003, *Market Opportunities in Homeland Security.*

Robotics Trends, September 06 and September 12, 2003. "Vender Spotlight – Security & Defense."

Technology Review, July/August 2003. "Monitoring Mom: As population matures, so do assisted-living technologies."

Traeger, Cynthia, 2002. "Biometrics Market Trends," Faulkner Information Services.