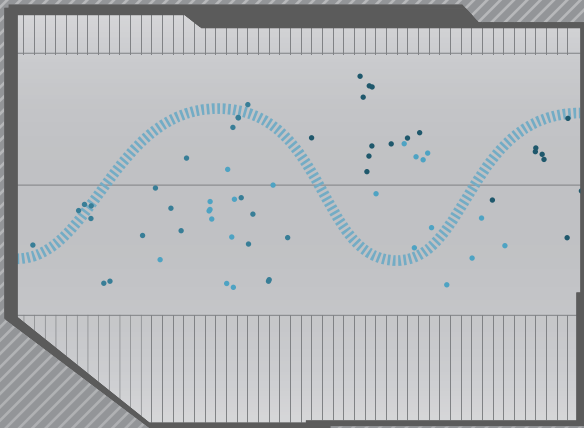


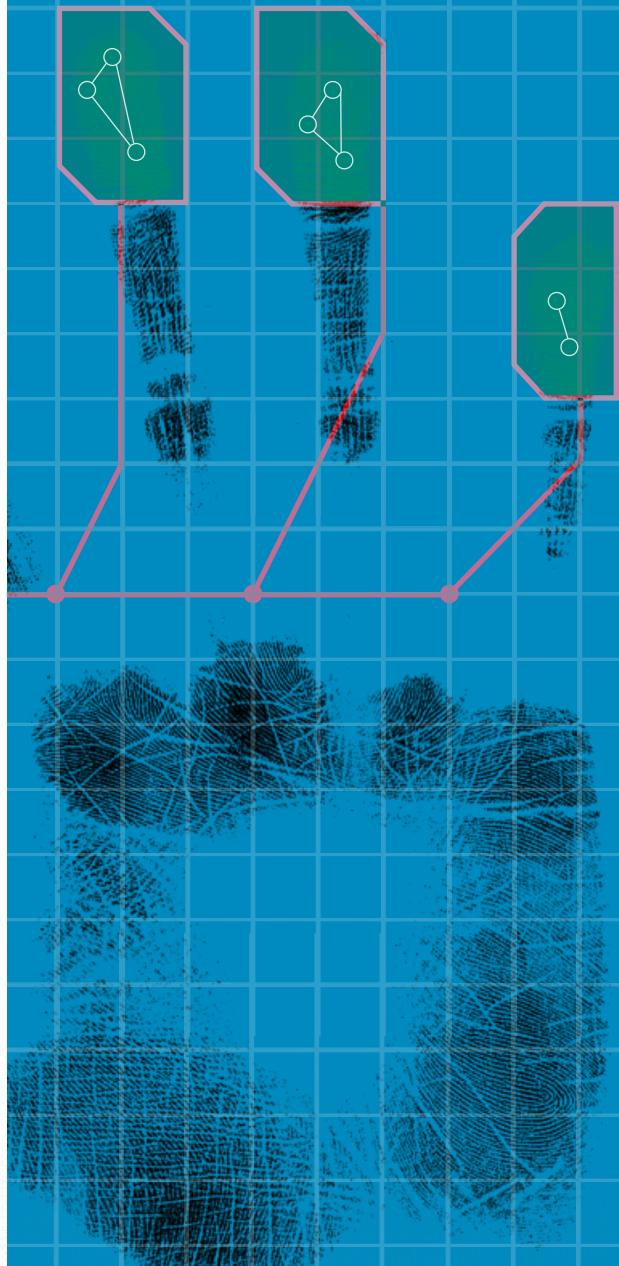

SECURITY
FORESIGHT

FUTURE ISSUE

BIO METRICS



*The Hague
Centre for
Strategic
Studies*



FUTURE ISSUE

BIOMETRICS

The Uncertainty
of Identification
& Authentication:
2010-2020

George Boone
Jonathan Huang
Stephan de Spiegeleire
Tim Swejjs

June - 2009

Contents

In Brief	3
The Big Picture	4
Meta-Analysis – Trends in Foresight Studies	6
Meta-Analysis – Parameters and Drivers	7
Robust Findings.....	9
Parameter/Driver Interactions	11
Future Scenarios.....	13
Security Implications and Applications	17
Basis of Biometric Applications	17
Framing the Analysis: Three Levels of Security	17
Relating the Scenarios to the Applications/Implications	22
Key Concepts for Security.....	23
Final Comments.....	27
Appendix A: Parameter Descriptions and Coding	28
Appendix B: Driver Definitions.....	29
Appendix C: List of Foresights and Endnotes.....	23
List of Foresights	31
Endnotes and Figure/Picture References	35

Figures

Figure 1	Percentage of Market Held by Various Biometric Technologies, 2007-2012	4
Figure 2	Biometric Growth by Continent, 2005-2010.....	5
Figure 3	Foresights by Publications Source, Year, and Percentage of Biometrics-Specific Studies ...	6
Figure 4	Meta-Analysis – Parameters.....	8
Figure 5	Meta-Analysis – Drivers.....	8
Figure 6	Relationship between Parameters and Drivers.....	9
Figure 7	Scenario Primal Instincts Prevail.....	13
Figure 8	Scenario Caged by Its Own Devices.....	14
Figure 9	Scenario Shedding the Security Blanket	15
Figure 10	Enhanced Security vs. Increased Risk Visualisation.....	26

Biometrics, the science and technology of measuring and analysing biological data, has become a hot topic within the emerging technology foresight literature. It has generated quite a bit of interest amongst security planning professionals. Global interest in biometrics has surged since 2000, and revenue projections for 2010 are expected to exceed 3.75 billion Euros.¹ Yet, there are many uncertainties that surround this technology and its place in the future. Will privacy or security be the prevailing factor in an individual's decision to use or avoid biometrics? Do biometric systems provide enhanced security? Based on an in-depth analysis of 58 publicly available foresight studies, this Future Issue addresses these questions and examines trends, drivers, and the future security dynamics in biometrics. Proponents contend that biometrics stands to offer enhanced security and/or greater convenience. Although the dissenters tend to agree with these assertions, they caution that significant privacy and identity theft issues could emerge from extensive use or over-reliance on biometrics technology, warning for the potential of biometrics to provide users with a false sense of security.

THE BIG PICTURE

PARAMETERS

Public Acceptance
Maturity/Reliability
Dominant Use
Market Breadth
Market Depth

DRIVERS

Security Concerns
Privacy Concerns
Demand for Convenience
Strategic Environment
Technological Convergence

SECURITY IMPLICATIONS

Biometric Divide
Identity Theft
Over-Reliance
Enhanced Security vs. Increased Risk

Figure 1 Percentage of Market Held by Various Biometric Technologies, 2007-2012²

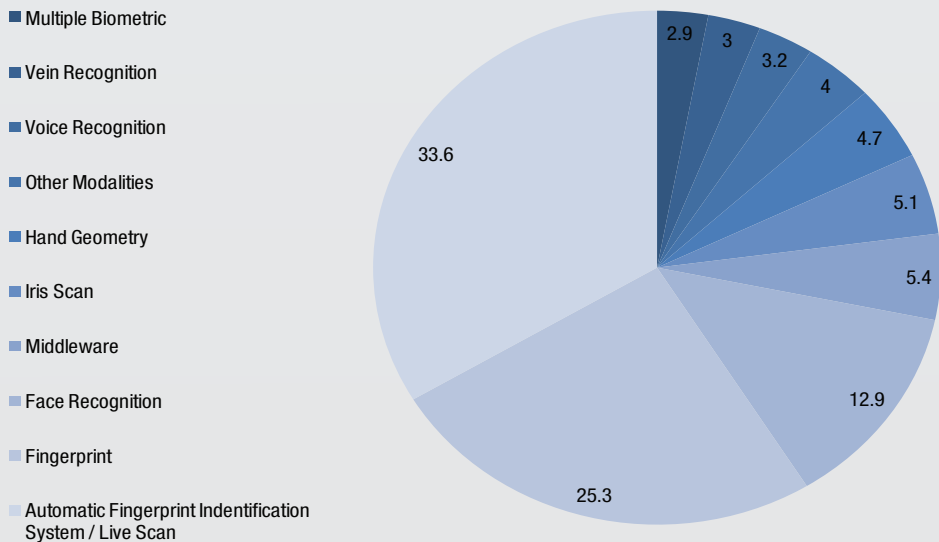


Figure 1: This figure shows that the simpler techniques (e.g. fingerprint) have a greater market share than the more technically intricate ones (e.g. multiple biometrics).

Biometrics, the science and technology of measuring and analysing biological data, is now a hot topic in technology foresight studies. Biometrics technology authenticates the identity of an individual by comparing scans of their unique physical attributes (e.g. fingerprints, iris, face, etc.) with millions of other records. This technology has become more practical recently, because information technology has progressed to the point that scans can be conducted and analysed in an efficient and effective manner. Presently, fingerprint-based biometrics is the most commonly used technology,³ and market projections through 2012 suggest that it will remain this way (as shown in Figure 1).

The biometrics market has nearly tripled since 2005. During this period, market growth (in terms of industry revenue) has remained fairly steady. However, as shown in Figure 2, the more technologically advanced areas of the world, the Global North, have experienced higher growth rates than those of the developing world, the Global South.

Figure 2 **Biometric Growth by Continent, 2005-2010⁴**

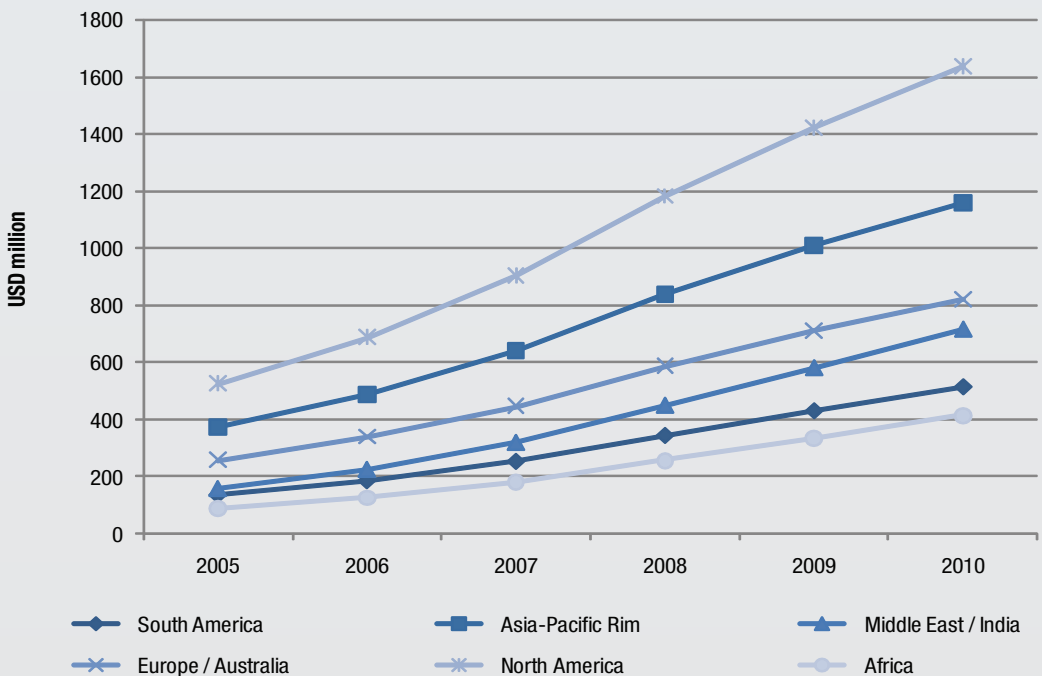


Figure 2: Growth rates for the geographical areas remained fairly constant, which leads to an increasing gap between North America and the rest of the world.

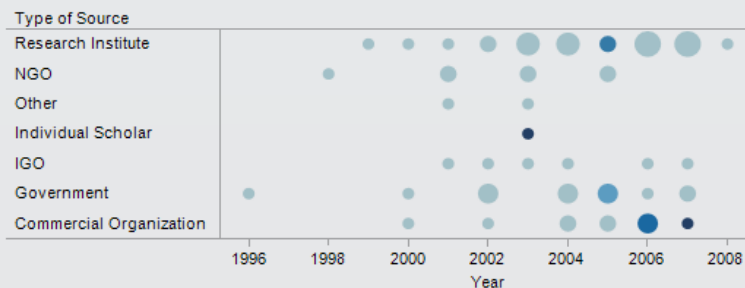
Despite these seemingly straightforward trends, there is quite some debate about the potential future use of biometrics. Proponents argue that it offers enhanced security. Opponents tend to agree with this assertion, but caution that significant privacy and identity theft issues could emerge from extensive use of biometrics technology.

Growing use of biometrics technology has security implications, both in a traditional and a nontraditional sense. In order to assess its potential impact, HCSS reviewed 58 foresights published since 1996, dealing with the future potential of biometrics technology between 2010 and 2020. The following analysis summarises the major insights in four main sections: 1) a meta-analysis of the foresight studies; 2) a combined evaluation of the main parameters (aspects of biometrics) of change over the next decade as well as the drivers fuelling those changes; 3) three potential biometric ‘future worlds’ and 4) an analysis of the security implications associated with emerging biometric applications.

Meta-Analysis - Trends in Foresight Studies

Looking at the interest in biometrics over time, an analysis of foresight studies reveals that biometrics did not become ‘mainstream’ until 2001 (see Figure 3).

Figure 3 Foresights by Publications Source, Year, and Percentage of Biometrics-Specific Studies



Prior to this, few foresights were written and no particular actor exhibited a serious interest in the subject. Since 2001, however, there has been a relative surge in the number of foresights produced on biometrics. The majority of these come from research institutions, but since 2004, those who would directly engage biometrics through policy choices or markets – IGOs, governments and commercial organisations, have increasingly looked at biometrics. Figure 3 shows that biometrics-specific foresights are a rather recent phenomenon. Besides the individual scholarly foresight in 2003, there was a lack of biometrics foresights prior to 2005.

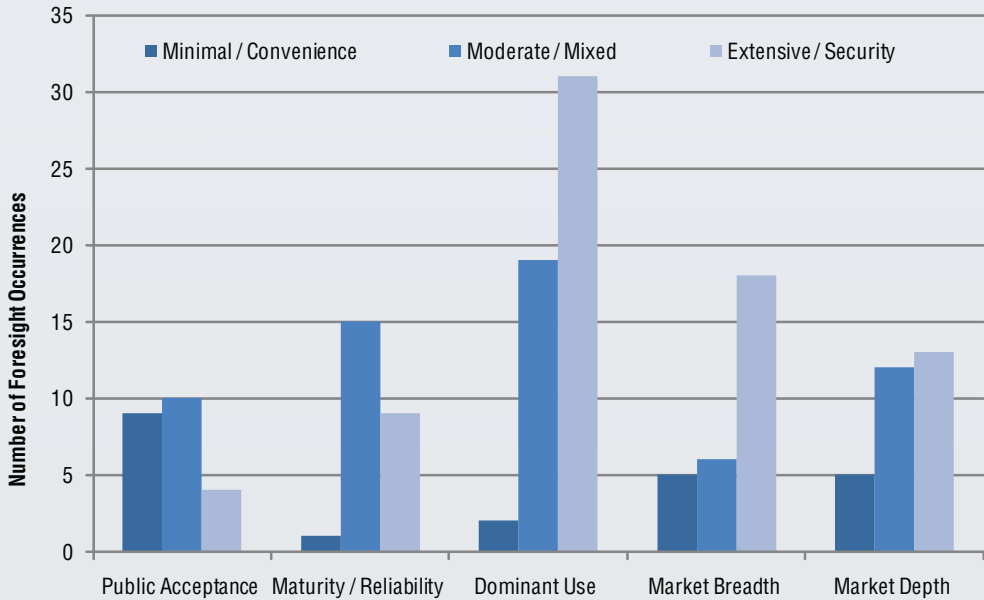
HCSS Assessment

The peaked interest in biometrics following 2001 was primarily prompted by the September 11th terrorist attacks. Given the traumatic impact of 9/11, the Western states turned to biometrics technology because it promised to offer enhanced security and a means of identifying 'bad guys'. The relative surge of biometrics-specific foresights primarily reflects the perception that biometrics had evolved from a supporting technology into one of greater importance. This is indicative of the slower iterative development process associated with biometrics (see Key Concepts for Security under the Security Implications section).

Meta-Analysis - Parameters and Drivers

The following section discusses the parameters and drivers found within the biometric foresights. Parameters are key aspects of a phenomenon that are subject to change over the next decade. In the case of biometrics five parameters were identified: public acceptance, maturity/reliability, dominant use, market breadth, and market depth. Public acceptance is the public's willingness to accept the risks associated with biometrics, whereas maturity/reliability concerns the expected degree of technological progress over the next decade. Dominant uses refer to the expected main use of biometrics (security or convenience purposes). Market breadth indicates the number of market sectors utilising biometrics technology, and market depth involves the level of penetration within these sectors.

When a driver or parameter occurred at a greater frequency, the resulting insight was considered to be robust (of higher quality and/or more reliable). Figure 4 shows a meta-analysis of the parameters, Figure 5 the drivers, and Figure 6 demonstrates the interactions between the drivers and the parameters.

Figure 4 **Meta-Analysis - Parameters**

Figures 4 & 5: Public acceptance, maturity/reliability, market breadth, and market depth are scored using the minimal/moderate/extensive scale, whereas dominant use is scored using the convenience/hybrid/security scale. Alternatively, in Figure 5, the drivers are scored based on how frequently they appeared in the foresights.

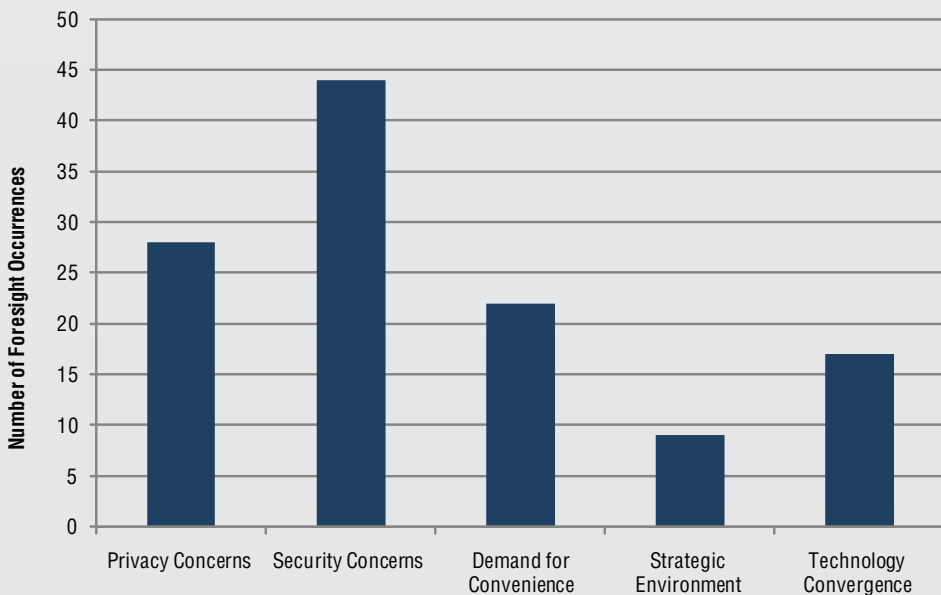
Figure 5 **Meta-Analysis - Drivers**

Figure 6 Relationship between Parameters and Drivers

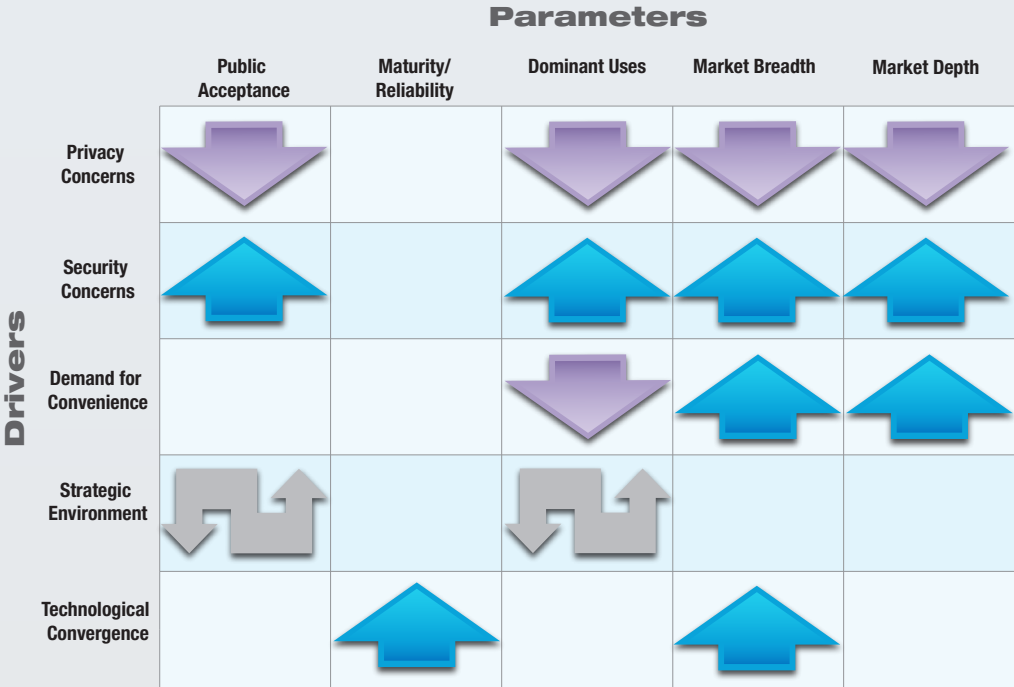


Figure 6: This diagram illustrates the interactions between the drivers and the parameters. The direction of the arrows indicates how the drivers impact the parameters. It should be noted that the double-headed grey arrows indicate that the driver can either have a positive or a negative impact.

Robust Findings

The foresights largely concur that biometrics will primarily be used for security-oriented purposes. For example, many of the foresights discuss the prospect of using biometrics to authenticate identities or to identify ‘wanted’ persons.

Our analysis of the drivers supports this finding. The foresights suggest that biometrics will be employed in one of three general uses: 1) security, 2) convenience (e.g. devices that adjust room settings in accordance with an individual’s preferences), or hybrid security/convenience (e.g. devices that remember passwords, based on a biometric key like fingerprint readers). Security concerns, such as the desire to prevent another terrorist attack, were considered to be a potential driver twice as often as the demand for convenience (76% of foresights vs. 37%). The foresights noted that privacy concerns, a moderately prevalent driving force (48% of foresights), had a deterrent impact on

those interested in biometrics for enhanced convenience, but mattered little for users focused on security. These concerns emerge because biometric data are susceptible to interception (e.g. hackers accessing a centralised biometrics database), and the fact that biometric identities cannot be replaced once compromised. From the preceding analysis, the following ‘hierarchy of potential motivators’ emerges in descending order: security, privacy, convenience. Forces driving a security-centric biometrics outcome are the most probable, whereas those propelling a convenience-oriented future are the least likely to occur.

The foresights agree that the biometrics market will encompass a number of different sectors, including defence, government and finance in the 2010–2020 time frame. Enhanced security (via biometrics) is a viable product in all market sectors. One foresight was entirely dedicated to how biometrics could improve security in the travel and leisure industry.

The market depth projections are hazier. Although 83% of the foresights consider market expansion in the sectors where biometrics has been introduced, they disagree over the extent to which these sectoral markets will grow. 40% percent of the foresights contend that it will be moderate, and another 43% percent maintain that it will be extensive. This ‘stalemate’ could reflect the uncertainty surrounding the impact that privacy concerns will have on the security-oriented biometrics market.

Similarly, the public acceptance parameter reveals a sense of uncertainty. The foresights seem to agree that the public will take a dim to neutral view of biometrics (84% of the foresights). This could in part stem from the increased privacy concerns associated with security-oriented biometrics. These applications tend to sacrifice items that are valuable to the individual (e.g. privacy, control, etc.) for enhanced communal security. For instance, face-imaging technology was used to sort through the fans at a recent Super Bowl in order to identify ‘persons of interest’. Critics would argue that the observers had no right to scan and identify the fans without their consent. It is important to note, however, that the volume of this type of criticism is moderated to some degree by the strategic environment. The foresights note that clear and direct threats induce the public to more readily accept socially intrusive technologies. For example, following the 9/11 terrorist attacks many Americans pushed for the passage of the Patriot Act and legislation enabling intelligence and police services to apply such measures as domestic wiretapping, which served to enhance anti-terror capabilities at the expense of civil liberties. On the other hand, individuals in strategic settings without such a menace are much less willing to accept the social costs associated with biometrics. Since the United States has not been attacked since 2001, the aforementioned tools have lost a

great deal of support, because many citizens are questioning the need for such intrusive measures when the strategic environment seems relatively calm. Therefore, with the foresights projecting a negative to neutral level of public acceptance, they appear to suggest that the increasing security-oriented nature of biometrics will create a body of criticism which cannot be effectively moderated by the strategic environment.

Finally, the maturity/reliability parameter appears to be fairly straightforward. The foresights suggest that biometrics technology will advance with moderate progress between 2010 and 2020. They more than likely settled on the middle ground owing to the somewhat limited nature of the technological convergence driver. Technological convergence simply notes how biometrics is affected by advancements and the synthesis of bio-, nano-, cognitive, and information technology. For instance, the hand-held biometrics scanning/identifying devices used by the US military not only required improvements in biological scanning technology, but also enhanced information processing technologies (storing and sorting through electronic records). Given that many advances in biometrics require a higher degree of technological convergence and that the foresights do not view this convergence as a prevalent driver, the moderate projections regarding technological maturity and reliability are understandable.

Parameter/Driver Interactions

Similar to public acceptance, the dominant uses parameter is also driven by the strategic environment. In a situation in which the general population perceives a high threat to its security, the strategic environment would reinforce the security-centric use of biometrics. Alternatively, the decreased 'perceived' need for security and inherent criticism associated with a more relaxed environment would facilitate a push towards convenience-based biometrics.

Along with security concerns, technological convergence and convenience also enhance market breadth. The former works to produce more and/or better applications that can be used in previously untapped market sectors. Furthermore, greater emphasis on convenience increases market breadth simply because of the heavy security-centric focus projected by the foresights.

Conversely, privacy concerns can limit market breadth. The logic for this relates back to the 'hierarchy of potential motivators' that the HCSS outlined earlier in this assessment (security, privacy, convenience). Privacy concerns could limit market breadth if the strategic environment is not in high threat mode. In this situation, only those sectors

of the market that absolutely require the security benefits (e.g. defence and homeland security) would seek to acquire biometrics, because privacy concerns would deter a great deal of the potential convenience-oriented users.

In terms of market depth, convenience/commercial demand serves as a positive driver. By targeting a different type of audience, convenience-oriented applications engage a different segment of the market.

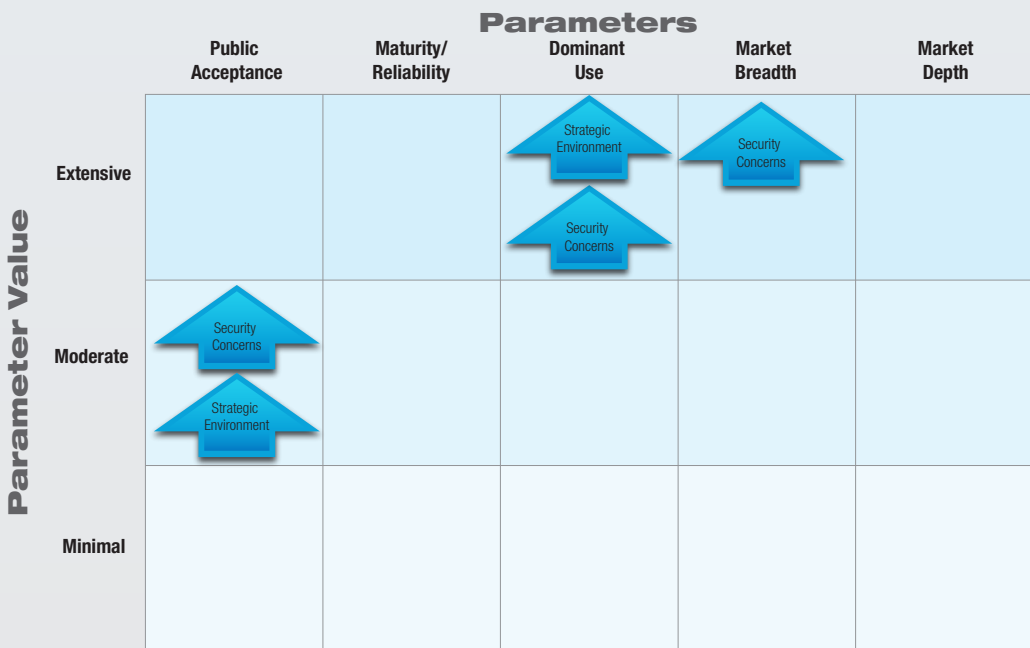
HCSS Assessment

Biometrics is inherently a multidisciplinary product, and its development will be highly reliant on progress in closely related technological disciplines (e.g. nano/bio/IT, etc.). The meta-analysis of available foresight studies suggests that 'security' looms all-powerful in the future of biometrics. HCSS wonders whether this 'robust' finding might not be a consequence of a clear security-bias in studies commissioned on biometrics after 9/11. We certainly see the potential for a sizeable commercially-driven biometric boom with large (and maybe unexpected) indirect implications for the security sector. We concur with the finding that privacy issues will play a key role in the future acceptance of such technologies, even if it remains uncertain which precise direction this debate will take.

FUTURE SCENARIOS

Using the findings from the previous section, HCSS developed three scenarios describing potential future 'biometric worlds'. Figures 7-9 are visual representations of these scenarios. These visualisations include the applicable interactions between the parameters and drivers. This is shown in Figure 6. The scenario descriptions follow each figure.

Figure 7 Scenario *Primal Instincts Prevail*



Primal instincts prevail is a future where society bandwagons on the security concept. In this scenario, there is a clearly defined and direct strategic threat (e.g. rise of a peer competitor, emergence of a regional challenger such as Iran, or re-emergence of catastrophic terrorism, etc.). The public becomes more favourable to biometrics and forgoes some of their privacy-based concerns in order to satisfy their security needs. In this situation, the public has little incentive to push for the development of non-security-related applications. As a result, aspects of biometrics research and development are neglected, which prevents the technology from reaching its full potential. Additionally, the public's security-centric mindset facilitates a broad biometrics market, because everyone (e.g. military/defence, travel & leisure, finance, etc.) is attempting to acquire instruments that will enhance security.

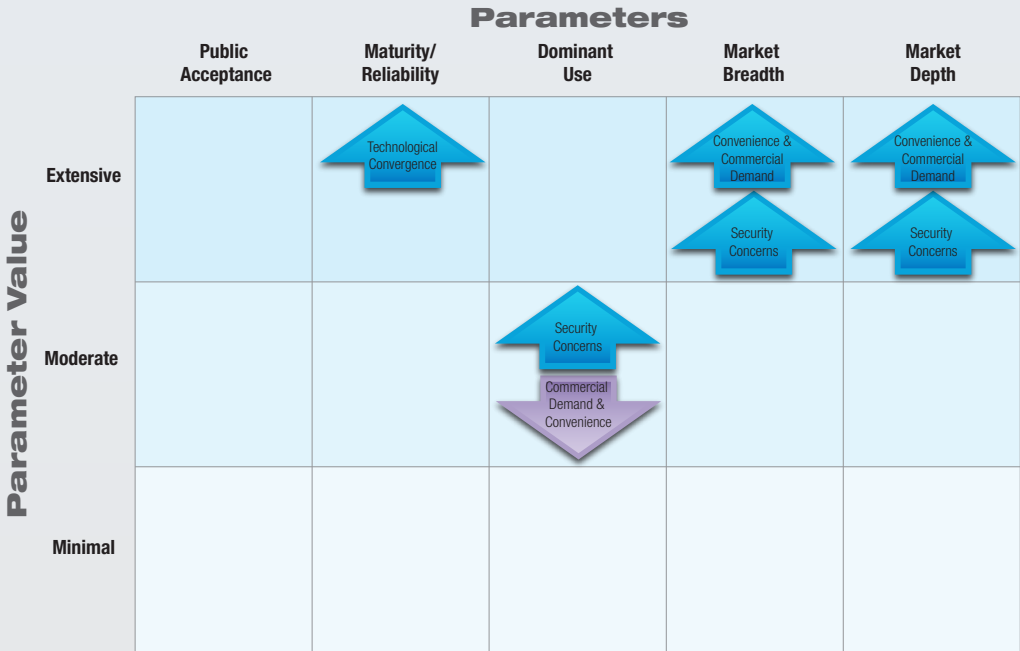
Figure 8 Scenario *Caged by Its Own Devices*

		Parameters				
		Public Acceptance	Maturity/Reliability	Dominant Use	Market Breadth	Market Depth
Parameter Value	Extensive			↑ Security Concerns		↑ Security Concerns
	Moderate					
	Minimal	↓ Strategic Environment ↓ Privacy Concerns			↓ Privacy Concerns	

Caged by its own devices is a security-centric biometrics future with limited overall market potential. This scenario hinges on two assumptions. First, the Western-oriented nations (primary users of biometrics) do not face a major direct threat (e.g. terrorism becomes a minor nuisance; energy prices drop and constrain ambitions of Russia and Iran; and India successfully counterbalances China). Second, the biometrics projects in the pipeline were initiated in a more security-centric period (e.g. post-9/11 in support of the Global War on Terror, Operation Iraqi Freedom and Operation Enduring Freedom) and thus primarily security-oriented. Without a direct strategic threat, society lacks a compelling incentive to rally around the flag and jump on the 'we want more security bandwagon'. Consequently, privacy and convenience become more important considerations. Since the public is primarily presented with security-oriented biometrics devices, there is little reason for them to accept these applications, especially since they inherently conflict with the desire for increased privacy. In the *Caged by its own devices* future, market depth will be extensive, but limited to a few sectors. Despite the reluctance of the general public to accept biometrics, certain security-minded sectors (e.g. defence/homeland security) will likely embrace it, because the technology enhances their capabilities. In light of the strategic situation, the security-centric focus of the applications in the pipeline, and the narrow customer base as well as their orientation (security), HCSS projects a future in which the orientation of biometrics towards security will be self-reinforcing. This accounts for the moderate degree of expected

progress in biometrics research and technology. Although history has shown that the military is willing to develop the technologies that spark its interest, concurrent civilian-oriented research has often provided a starting place and key insights. Therefore, given the lack of civilian biometrics output projected in this scenario, one cannot expect that biometrics technology will progress at the maximum potential rate.

Figure 9 Scenario *Shedding the Security Blanket*



Shedding the security blanket represents a fairly bright biometrics future. This scenario is based on two assumptions. The first is the same as in *Caged by its own devices* – no perceived direct threat. The second is that the post-9/11 security-oriented mindset of the Western public moderately relaxes/degrades over time. As a result, some convenience-based or hybrid convenience-security-based applications enter the research pipeline. In this scenario, non-security-oriented biometrics applications will enter the market between 2010 and 2020. Consequently, the increased diversity of applications should have a positive impact on public acceptance. The introduction of more convenience-based biometric products should not only serve to soften the technology’s image but also better align biometrics with the public’s interest. Given the increased range of applications and public support, biometrics technology should appeal to more market sectors than those primarily focused on security. Furthermore, enhanced product diversity enables biometrics to become further integrated into a market sector (e.g. travel & leisure: (1) security – identification of terrorists/wanted persons at check-in, (2)

convenience/security – fingerprint-enabled door locks (no worries about keys), and (3) convenience – lighting, temperature, and entertainment preferences facilitated upon entering a room). Finally, this future involves a high degree of technical maturity. This is possible due to the wide variety of research originally in the pipeline (military & civilian and for purposes) as well as increased public support, and thus continued research, for biometrics.

Basis of Biometric Applications

The majority of the foresights consider that in the future, biometric technologies will use a few human physical characteristics, in particular fingerprint and palm print verification, iris scan and retina analysis, face and voice recognition, and hand geometry. For most of these, the technologies already exist today. In certain studies, signature dynamics are also considered as a biometric. Some of the more advanced proposals of biometrics include personal odour, the remote applications of existing technologies (i.e. remote facial recognition), and DNA and other genetics-based identification and profiling. However, at present most foresights do not consider DNA and genetics-based identification as a viable biometric, for its long processing time does not allow for real-time response (an important aspect of most biometric applications).

Framing the Analysis: Three Levels of Security

The biometric-based security applications found in the foresights can be roughly divided into three categories. The first category concerns interstate or homeland security intrastate security. It involves applications that can be used at the international and the domestic level, having implications for strategic interactions between states and homeland security. An example is biometrics used for border control. The second category concerns biometric applications used by institutions and commercial ventures, such as businesses, banks, and others. An example is the smart credit card that employs biometrics as additional security for transactions. The third category relates to individual and human security, which concerns the health, privacy, and safety of individuals. An example of a biometrics security application in this category includes biometric tags used as identifiers for healthcare purposes.

The security applications and relevant implications are presented in the following chart, describing the use of biometric applications, their security implications, where possible the projected time frame, and whether a certain technology or application of a technology already exists. Where there is no specific information on the time projection of specific applications, the time frame is indicated as 'not clear' in the chart.

	CONCEPTUAL USE	TECHNICAL APPLICATION	IMPLICATION	TIME ESTIMATE
INTRASTATE / HOMELAND SECURITY	Access Control	Biometric-Based Keys to Military Assets	Biometrics can be used as "keys" that provide and control access to critical military assets such as tanks, aircrafts, or weapons. This may also mean that the access of certain military assets can become more personalised and better tracked, ensuring a greater degree of security.	Not Clear
		Biometric Identification System for Access (BISA)	Biometrics used to ensure that a person entering a facility (such as a military base) is not included in the U.S. databases of known terrorists and suspected enemy combatants. By using biometrics, this technology ensures that facilities and sensitive areas are more secure against intrusion, providing great value to places like military bases in conflict zones.	Technology currently exists. Future level of use unclear.
		Defense Biometrics Identification System (DBIDS)	Biometrics, such as fingerprints or hand geometry, used to identify personnel entering military installations. By using biometrics, the access process is quicker and lower the chance of human error by checking the person against a photo ID. In addition, this technology using biometrics can also assign different levels of access, allowing for classification in access and further preventing faulty permission to enter sensitive areas or facilities.	Technology currently exists. Future level of use unclear.
	Authentication	Biometrics-Enhanced User Interfaces (Facial, Iris, Fingerprints)	Biometrics can be used in regular machine-human interface and can provide better measures for verification and authentication. Biometric enhanced authentication can potentially provide better protection to sensitive information and materials.	Technology currently exists. Future level of use unclear.
	Automated Screening	Remote Biometric Sensing	Biometrics can provide a means throughout which screening of people can become an automated process, thereby reduce the infrastructure costs and reduce potential human mistakes.	2015
	Border Patrol	Biometrics-Enhanced Passports (Iris Scanning, Smart Cards, etc)	Biometric characteristics, such as fingerprints and iris scans, can be incorporated with a person's passport, and this can enhance the level of verification for the purpose of border patrol. However, the different level of implementation of biometrics-enhanced documentation can create a technological divide between countries that are capable of employing biometrics and those that cannot, creating potential friction and tension between states.	2015
		Facial Recognition and Temperature Scanning	Biometrics such as facial recognition and temperature scanning can be used as additional measures in border patrol to help identify terrorists passing through, for example, an airport, or prevent the spread of communicable disease (i.e. during SARS, temperature scanning is employed to identify those passengers who have a fever).	Not Clear

	CONCEPTUAL USE	TECHNICAL APPLICATION	IMPLICATION	TIME ESTIMATE
INTRASTATE / HOMELAND SECURITY	Information Collection / Processing / Storage	Automated Biometric Identification System (ABIS)	Modeling after existing fingerprint identification system, this biometric technology consolidates, stores, and searches these data. This can create a biometric database that allows for strengthened access control, authentication, and surveillance.	Technology currently developing. Future level of use unclear.
		Biometrics Automated Toolset (BAT)	A toolset (computer system) that incorporates biometric scanners that is developed for identifying people and make records of individuals' identity via biometrics. This application has provided great utility to the military, particularly for the soldiers in conflict areas where being able to tell between innocents and enemies is critical.	Technology currently exists. Future level of use unclear.
		Hand-Held Interagency Identity Detection Equipment (HIIDE)	Hand-Held devices that enroll, match, and verify persons with biometric data from iris scan, fingerprint, and facial recognition. The portability of this device increases the flexibility and allows for its use in the field.	Technology currently exists. Future level of use unclear.
		Intelligent Information Systems	Advanced biometrics can be used to create an intelligent information system in which people's data can be automatically collected, processed, and stored. This will enhance the ability and efficiency of the government to collect and process vital information of its citizens.	Not Clear
	Monitoring / Surveillance / Tracking	Centralized Biometric Databases	Biometric databases of criminals can be created and distributed by government to local businesses (such as hotels, vendors, etc.) to increase operational efficiency of tracking and keeping a record of the movement or action of a criminal.	Not Clear
		Genetic Profile Scanner	Biometrics may provide a means through which the genetic profile of a person can be identified and used for the purpose of tracking and surveillance. The citizens will have less ability to hide their identity from the government, shifting the power balance between people and government to government's favor.	2020
		Iris on the Move	Biometric technology such as remote iris scanning can be used for tracking a person. This can enhance processing time and ease of tracking and monitoring of people.	Not Clear
		Using Biometrics in a Similar Fashion as RFID for Tagging	Biometrics can be used as a tagging device (function in a similar way as RFID), and this can be used to keep track of criminals and monitor their movements. This can help to enhance the level of public safety.	2015
	Smart Uniform	Biometric Sensors	Biometrics can be incorporated in uniforms that can sense the physical conditions of a person and such information can be related to the command centers for a better accounting of personnel. This can potentially be used both militarily and commercially, but existing considerations are more heavily military-focused.	Not Clear

	CONCEPTUAL USE	TECHNICAL APPLICATION	IMPLICATION	TIME ESTIMATE
INSTITUTIONAL / COMMERCIAL SECURITY	Access Control	Ambient Intelligence Space	Biometrics, when combined with other sensor technologies, can create intelligent spaces in which a person's identity can be authenticated without the need of physical access control (such as a lock). This will eliminate the need to use physical keys, reduce the associated risk, and increase the convenience.	2015-2020
		Iris Scanning	Biometrics can provide better control of access to the information and materials that need secure access.	Technology currently exists. Future level of use unclear.
	Access Convenience - Authorized Users Only	Biometric Touch Sensors	Biometrics can provide secure and easy access to a shared computing or information environment without the need of passwords. This can help reduce the security risk of using passwords and can better keep track of access.	Not Clear
	Enhanced Employee / Client Authentication	Biometrics-Enhanced Smart Cards	Cards can incorporate biometrics as an authentication method. When the card is used, the user's bioidentity can be checked against the one stored in the card. This can provide extra layer of security for commercial transactions and a verification measure that is event-driven.	Not Clear
		Finger Geometry Based Check Out System	Biometrics such as finger geometry can be used as a means of authentication that facilitates identification of the client and processing time in a close environment (i.e. a resort). This can enhance the convenience by eliminating the need to carry around things such as IDs or Credit Cards.	Not Clear
		Iris on the Move	Biometric technology such as remote iris scanning can be used for enhancing processing time and payment applications for merchants.	Not Clear
	Tracking and Surveillance of Employees	Iris Recognition	By using iris scanning and recognition technologies to track employee actions and movements, employers can improve work schedule, streamline procedures, and better monitor employee's health and safety.	Not Clear

	CONCEPTUAL USE	TECHNICAL APPLICATION	IMPLICATION	TIME ESTIMATE
INDIVIDUAL / HUMAN SECURITY	Additional Verification	Using Biometrics as Additional Verification Protocol	Biometrics can be used as an additional verification measure for one's identity. This can enhance the security of one's identity.	Application currently exists. Future level of use unclear.
	Healthcare and Safety	Biometric Sensors	Biometric-enabled sensors can be used medically to providing advanced diagnostics for patients.	Not Clear
		Biometric Tags	Biometric tags can be used as code keys. They can also be used as personal identifiers for patients and for other health-related uses that are only activated when needed.	2015
	Identity Theft	All Biometric Technology (except smart card assisted)	Criminals may use biometrics-based technologies to steal individuals identity -- thus complicating verification procedures. Biometric identities cannot be replaced as is the case with 'regular' identity cards.	Not Clear
	Privacy Enhancement	Smart Cards	Biometric-enabled cards can in fact be privacy-enhancing. A card (i.e. credit card) that is biometrically tied to its owner enhances the level of privacy by transferring the risk of loss of privacy and identity to the actual card holder.	Not Clear
	Single ID	Biometrics as the Sole ID	Advanced biometrics may be used as the sole form of identification for a person.	Not Clear

Note - Text in black is derived inductively from the foresights; text in blue is included from HCSS deductive assessment

Interstate/Homeland Security

In general, at the interstate/intrastate level, biometric applications are employed to enhance security, amongst others through access control, identity authentication, and tracking/ surveillance. Developments in information collection/processing/storage will help to increase the practical use of biometrics for security purposes. For example, the Automated Biometric Identification System (ABIS) consolidates and stores biometric data in a central location, enabling faster processing times for those who need to verify an identity.

Institutional/Commercial Security

At the institutional/commercial level, biometrics is employed in a dual-use capacity: security mixed with convenience. At the commercial/institutional level, the goal is to run a business efficiently and effectively. This requires some semblance of security,

but draconian measures may have an adverse impact on productivity. Alternatively, convenience-based applications would greatly enhance efficiency and effectiveness, but may promote an excessively open atmosphere and jeopardise monetary transfers and product confidentiality. As such, this level represents a happy medium between the two. In fact, five of the seven emerging applications in the institutional/commercial realm were designed for a hybrid security/convenience use.

Human/Individual Security

Biometrics at the human/individual level generally seeks to enhance the security of the individual. Emphasis is placed on protecting privacy and enhancing medical care.

Relating the Scenarios to the Applications/Implications

What do these technical applications and relevant security implications mean for the three possible future scenarios of biometrics? The Primal instincts prevail world favours biometric applications that enhance border control, automated screening, and surveillance and monitoring. Technologies such as biometrics-based passports and a centralised biometric database or advances in genetic and facial recognition technologies will receive high priority and attention from the government and the public alike. In the Caged by its own devices scenario, where a direct threat is not widely perceived and public acceptance of the use of biometrics is low, applications that focus on access control, authentication and verification will be pursued in selected sectors where security needs to be enhanced. Technologies such as biometric-based keys or user interfaces will be used, but the market for such technologies will not be wide. In the Shedding the security blanket world biometrics will achieve a high level of acceptance and market penetration in government and commercial sectors alike. As a result, in addition to the authentication- and verification-based biometric security technologies, other developments for the sake of convenience, such as biometrics for medical use, biometric smart cards, and ambient intelligence space will be developed.

Biometrics and Nanotechnology Are Fundamentally Different Emerging Technologies

The Future Issue on Nanotechnology, published in 2008, noted that nanotechnology had the potential to revolutionise society and the security realm (deterrence, arms acquisition, etc.). Biometrics takes a much shorter leap. Many of the expected developments in biometrics are being facilitated by the application of old technologies in new ways (e.g. iris scanning to monitor the health/safety of miners). Furthermore, biometric developments using new technology are designed to improve an existing capability. In fact, there is a lack of developing new technologies to do new things. Biometrics is developing by short incremental steps, and as such has different implications for the security realm than nanotechnology.

Biometric Divide

The emphasis placed on security-based applications at the interstate/intrastate level enhances the problem of the biometric divide. Recall that Figure 2 depicted the biometrics markets by continent. In this graph, there was a clear distinction between the Global North and Global South. If countries with larger biometrics markets pursue security-based applications, while the less developed countries invest relatively little in biometrics, this will create a technological rift with security implications. If the Global South has not collected biometric data from its citizens, then the investment made by the Global North will have relatively little impact except for domestic surveillance and Global North-based enemies (e.g. Al-Qaeda terrorists in Germany). This is problematic, because many threats to biometrics-enabled countries originate in the Global South (e.g. terrorists, drug traffickers, etc.). As such, the potential defensive enhancements offered by biometrics cannot be fully realised. Therefore, in order for the Global North to make the best use of its biometric capabilities, it must work to decrease the biometric divide amongst states and increase the divide between states and non-state actors.

Identity Theft

The development of biometrics technology has the ability to make identity theft a much more attractive pursuit. Biometric data appear to provide the ideal means of identity verification, because they are unique and permanently attached to their owner. The downside, however, is that once biometric data are stolen they cannot be replaced. If a criminal obtains someone's fingerprint data, the victim's identity is permanently compromised, because they cannot generate a new unique access code and the system lacks the ability to discern between the code used by the criminal and the victim. State actors have already initiated programmes to construct centralised biometric databases (e.g. United States Department of Defense – Automated Biometric Identification System) that do not require the use of smart cards, items held by an individual to ensure that biometric data are accessed only with their consent. Since these databases would be communicating with devices in the field, this opens the prospect for someone to hack the system.

Over-Reliance

As the reliability of biometrics increases and people grow accustomed to the convenience offered by the technology (e.g. no passwords to remember), over-reliance on biometric-based security may become an issue. If people become comfortable with biometrics, they may feel that their highly complex individualised key offers ample security and, as a result, resort to guarding their valuables solely with biometric codes. This is unwarranted, as biometric keys are not entirely secure. Therefore, over-reliance on biometric security would serve to further degrade the real defensive gains offered by the technology.

Enhanced Security vs. Increased Risk

The basic trade-off associated with biometrics involves enhanced security for increased risk. This concept is explained in the following section and visualised in Figure 10.

Under normal conditions, biometric devices provide enhanced security. They are genuinely unique keys, which are difficult to replicate and in most cases are permanently attached to their owners (e.g. iris). If systems use these secure individualised keys to facilitate sensitive functions, this will increase the system's ability to prevent unauthor-

ised access/use, and consequently, augment overall security. The defensive benefits afforded by a biometric system relative to a non-biometric system can be seen in Figure 10, showing that user and administrator confidence in system security would surge due to the gains offered by biometrics.

Despite the sense of security derived from biometrics, there are rather undesirable side effects, including increased risk. Biometrics data are vulnerable to theft. Two forms, fingerprints (through trace elements left after contact) and DNA (hair follicles) can be acquired with relative ease. Furthermore, biometric keys can be stolen from their owners (e.g. violent and criminal acquisition of body parts – reference the James Bond motion picture *Die Another Day*), and hackers can intercept the data that are used to satisfy web-based biometrics security systems. An illegitimate user could obtain a key and gain full access without alerting the security system. A mass attack (i.e. near-simultaneous use of several compromised keys) would surely result in at least one successful entry, because biometric systems are highly accurate, in excess of 99%, and the probability of multiple errors is nearly zero. However, even if the system realises that it has been breached, it could not deny the intruder access without doing the same for the compromised authorised user, because the two are using the same key and the latter lacks the ability to change his/her password (e.g. cannot grow a new unique iris). Therefore, non-biometric systems are less secure but easier to fix, whereas biometric systems offer greater security but have much longer and difficult recovery periods following an attack (Figure 10).

Figure 10 Enhanced Security vs. Increased Risk Visualisation

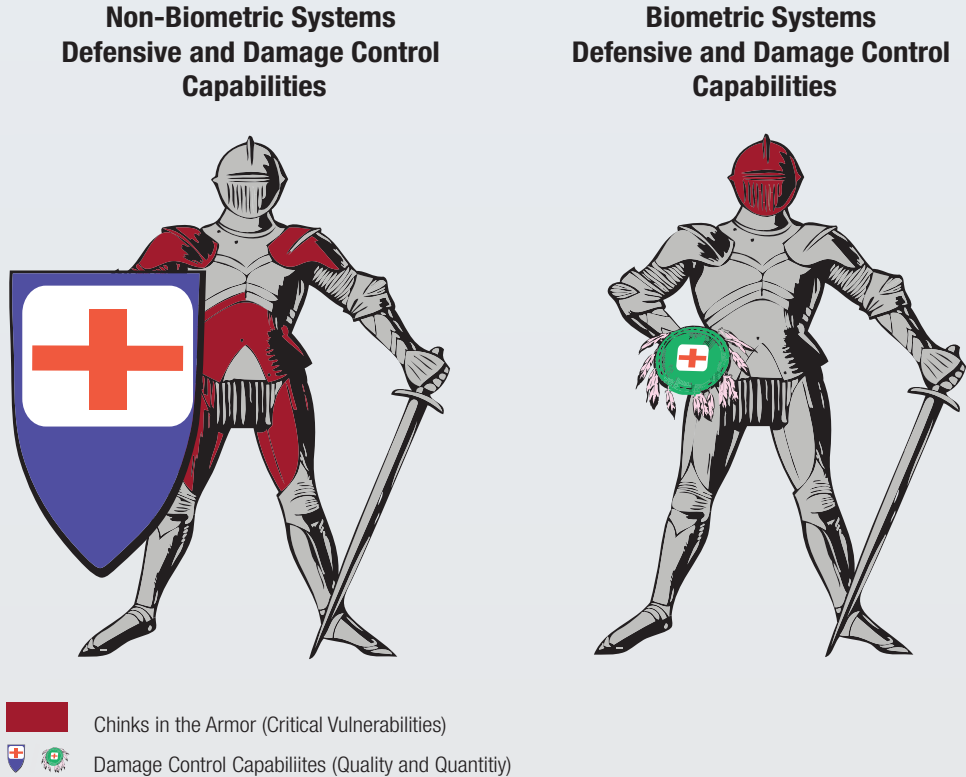


Figure-10: This figure uses the chink in the armor concept to illustrate the differences in the level of security and risk between non-biometric and biometric systems. HCSS has operationalized system vulnerability as the quantity of chinks in the armor. As the figure demonstrates, the non-biometric systems are more vulnerable on account of the fact that they employ inferior front-end security systems. Alternatively, the shields carried by the knights are proportional representations of each system's damage control capabilities. The non-biometric system has greater damage control/recovery capabilities (large iron shield as opposed to small leather shield), because it is more sensitive to unauthorized access and it has the ability to lock out unauthorized users after a breach. Although biometrics-enabled security systems will facilitate fewer breaches overall, these breaches will be more costly than those achieved on non-biometric systems due to the lack of back-end support (damage control capabilities). Therefore, increased security on the front-end comes at a definite cost.

FINAL COMMENTS

Irrespective of its dominant use, HCSS sees a bright future for biometrics – both in its civilian AND in its security applications. We anticipate that biometrics will become a standard tool for security sectors around the world. Yet, we also want to draw public and private decision makers' attention to two points that we feel are insufficiently covered in the foresight studies.

1. Biometrics is unlikely ever to prove the panacea many advocates suggest it will become.
 - o The international community will never fully reap the rewards of its investment in biometrics unless the biometric divide between the 'Global North' and the 'Global South' is bridged – which will prove extremely difficult.
 - o There is a risk that biometrics may lull states into a false sense of confidence in their defences, thus emboldening offensive actors (e.g. hackers, identity thieves, etc.) to find chinks in the armor and to tip the offence/defence balance in their favour.
2. The problem of over-reliance could be alleviated by the use of a second non-biometric key. Although the convenience factor would be reduced, this would address one of the major flaws in biometric security, the back-end capabilities, and offer enhanced security, albeit at a slightly higher cost.

Public Acceptance

The public's willingness to accept the risks associated with the advancements in biometrics. Public acceptance is coded on a scale from unwilling to willing.

Operationalisation: 1 = unwilling; 2 = indifferent; 3 = willing

Maturity/Reliability

The degree to which technological progress in biometrics will be made in a given time frame. The more advanced the technology, the more reliable it will become.

Operationalisation: 1 = minimal progress; 2 = moderate progress; 3 = highly advanced progress

Dominant Uses

The main use of biometrics. This parameter is coded from convenience to security as the main purpose of the technology.

Operationalisation: 1 = primarily for convenience; 2 = for both; 3 = primarily for security

Market Breadth

The market spread of the biometrics-based technologies. Biometrics may be adapted only in very few selected industries, or it could be used widely by many different social and industrial sectors. This parameter is coded from narrow to wide.

Operationalisation: 1 = narrow; 2 = moderate; 3 = wide

Market Depth

The level of market penetration of biometrics-based technologies. Biometrics may be integrated into society and the market at a very shallow level (meaning it is used minimally), or it can be so deeply ingrained that it becomes the predominant measure of identification and security. This parameter is coded from minimal to extensive.

Operationalisation: 1 = minimal; 2 = moderate; 3 = extensive

DRIVER DEFINITIONS B

Privacy Concerns

The use of physical information of a person by biometric applications may be regarded as a form of privacy invasion, which raises concerns among the public. Privacy concerns may limit the level of public acceptance, which may in turn affect the development of specific biometric technologies that are considered too invasive. A high-level concern for privacy may also limit the level of market width and breadth.

Security Concerns

Biometrics R&D is driven by concern for security of information, secure identity verification and control of access. Concern for security of information will drive the dominant use of biometrics towards a security-oriented use. Security concerns may influence the breadth and depth of a biometric application's market penetration (i.e. if the security concern is very high, and the biometric applications can provide the best kind of security of information, the market sectors that will need to adopt biometrics as a form of protection may be limited, but their use will penetrate that sector at multiple levels).

Convenience/Commercial Demand

Biometrics R&D is driven in part by the convenience it is expected to bring (whether as a deliberate goal or as an unintended by-product). Just like the security concern driver, commercial demand for convenience may drive the dominant use of biometrics towards convenience rather than security. A commercial demand for convenience may affect the breadth and depth of a biometric application's market penetration (i.e. if biometric applications are developed for convenience's sake, they may reach out to more sectors of the market, while their use may only be applied at a surface level).

Strategic Environment

Changes in the strategic environment, such as an event similar to 9/11, can influence the projected direction of development of biometrics. It may prompt the public to becoming more open to the use of biometrics for security purposes, whereas a relaxed strategic environment may reduce such potential.

Technology Convergence

The R&D in biometrics impacts the increasing trend of technological convergence. The convergence of bio-/nano-/cogno-/information technologies may affect the degree to which biometric applications will be reliable and widely used, and can, as a result, indirectly influence the width and depth of the market penetration that biometrics may enjoy.

List of Foresights

“2003: Ten-Year Forecast.” Institute for the Future, 2003. http://www.iff.org/system/files/deliverables/2003_Ten-Year_Forecast.pdf.

“21st Century Defense Technologies.” Defense Science Board, 1999. <http://www.acq.osd.mil/dsb/reports/ninetyninesummerstudy.pdf>.

Andreas Ligtoet. “Prisma Strategic Guideline 2: eHealth .” PRISMA, 2003.

Anette Braun, Anastasia Constantelou, Vasiliki Karounou, Andreas Ligtoet, Jean-Claude Burgelman, and Marcelino Cabrera. “eHealth in the Context of a European Ageing Society: A Prospective Study.” European Commission, 2004.

Barbara Daskala and Ioannis Maghiros. “D1gital Territ0ries .” European Commission, 2007.

Bart Van Looy, Koenraad Debackere, Petra Andries, Edwin Zimmerman, Julie Callaert, and Arnold Verbeek. “Technologies for the Future: Looking a Decade Ahead.” Agoria Vlaanderen, 2001. http://www.vrwb.be/MFiles/Technologies_for_the_future.pdf.

Bastian Giegerich, Jennifer Azari, and Raffaello Pantucci. “FORESEC Deliverable D 2.2 Country Report on Germany,” 2008. http://www.foresec.eu/wp2_docs/Germany.pdf.

“Biometrics Technology Roadmap for Person Identification within the Police Service .” Police IT Organization, 2005. http://www.npia.police.uk/en/docs/PITO_ID_Roadmap_2005_Part_1_vFinal_1.1.pdf.

“Biotechnologies to 2025.” Ministry of Science and Technology - New Zealand, 2005. <http://www.morst.govt.nz/Documents/work/biotech/FutureWatch-Biotechnologies-to-2025.pdf>.

Bluepeter Management Consulting and Access Market International. “South African Benchmark 2020 .” South African Department of Trade and Industry, 2004.

Charlie Edwards and Paul Skidmore. “A Force for Change: Policing 2020.” Demos , 2006.

Clara Centeno. “Securing Internet Payments: The Potential of Public Key Cryptography, Public Key Infrastructure and Digital Signatures .” European Commission, 2002. <ftp://ftp.jrc.es/pub/EURdoc/eur20263en.pdf>.

“Crime Prevention Panel .” Foresight , 2000.

Edward F. Murphy, Gary C. Bender, Larry J. Schaefer, Michael M. Shepard, Charles W. Williamson III. “Information Operations: Wisdom Warfare for 2025 .” United States Air Force , 1996. <http://csat.au.af.mil/2025/volume1/vol1ch01.pdf>.

Frank Simonis and Steven Schilthuizen. “Nanotechnology: Innovation Opportunities for Tomorrow’s Defense .” TNO, 2006.

“Future Bottlenecks in the Information Society .” European Commission, 2001.

“Future of Biometrics .” Biometric Technology Today, 2007. http://www.sciencedirect.com/www.library.gatech.edu:2048/science?_ob=MIimg&_imagekey=B6W70-4NJXN-SY-J-7&_cdi=6612&_user=655052&_orig=search&_coverDate=04%2F30%2F2007&_sk=999849995&view=c&wchp=dGLbVlz-zSkzk&md5=307ed2b3068630bb9024d7de17bbed30&ie=/sdarticle.pdf.

Graeme Newman and Ronald V. Clarke. “Etailing: New Opportunities for Crime, New Opportunities for Prevention.” Office of Science and Technology - United Kingdom, 2002.

“Industrial Priorities for Human Factors Research in UK Defence and Aerospace ,” 2002.

J. Millard, R. Warren, C. Leitner, and J. Shahin. “Towards the eGovernment Vision for the EU in 2010: Research Policy Challenges .” European Commission, 2006.

Jim Wayman. “The Past and Present Future of Biometrics ” presented at the Presentation to the Biometrics Institute, Sydney, Australia, August 1, 2003. <http://www.barcode.ro/tutorials/biometrics/futureofbiometrics.pdf>.

“Joint Urban Operations - Joint Integrating Concept.” United States Department of Defense , 2007. http://www.dtic.mil/futurejointwarfare/concepts/juo_jic_v1.pdf.

K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, and J-C. Burgelman. “Scenarios for Ambient Intelligence in 2010.” European Commission, 2001. <ftp://ftp.cordis.lu/pub/ist/docs/istagscenarios2010.pdf>.

“Key Factors Driving the Future Information Society in the European Research Area,” 2004. <ftp://ftp.jrc.es/pub/EURdoc/21310-ExeSumm.pdf>.

“Living Tomorrow: Information and Communications Technology in Germany in 2015 .” RAND, 2005.

Maarten Botterman, Jonathan Cave, James P. Kahan, Neil Robinson, Rebecca Shoob, Robert Thomson, and Lorenzo Valeri. “Cyber Trust and Crime Prevention Project - Gain-

ing Insight from Three Different Futures ." Office of Science and Technology - United Kingdom, 2004. <http://www.berr.gov.uk/files/file15325.pdf>.

"Manufacturing and Crime," 2001.

"Mapping the Global Future ." United Kingdom National Intelligence Council, 2004.

Marc van Lieshout, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Thijs Veugen, Bram van der Waaij, and Claudio Borean. "RFID Technologies: Emerging Issues, Challenges, and Policy Options ." European Commission, 2007. <http://www.stop-project.eu/portals/1/publications/eur22770en.pdf>.

Matthew Meyers and Juline E. Mills. "CERIAS Tech Report 2005-2007." Center for Education and Research in Information Assurance and Security, 2003. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-07.pdf.

Michael Friedewald and Olivier Da Costa. "Science and Technology Roadmapping: Ambient Intelligence in Everyday Life," 2003. http://forera.jrc.ec.europa.eu/documents/SandT_roadmapping.pdf.

Mike Tuller, Alok Dhawan, Bob Simon, Khai Lee, and Dan Ward. "Biometrics: Strategic Technology Analysis."

PA Consulting. "Biometrics," 2006. http://www.paconsulting.com/NR/rdonlyres/8C70168E-B730-4906-BAB7-356961361FFE/0/foresight_biometrics.pdf.

Philip S. Anton, Richard Silberglitt, and James Schneider . "The Global Technology Revolution: Bio/Nano/Materials Trends and Their Synergies with Information Technology by 2015." RAND, 2001.

Rachel Briggs. "Joining Forces: From National Security to Networked Security ." Demos, 2005.

Richard Silberglitt, Philip S. Anton, David R. Howell, and Anny Wong. "The Global Technology Revolution 2020: In-Depth Analysis ." RAND, 2006.

Robert Phaal. "Foresight Vehicle Technology Roadmap." United Kingdom Department of Trade and Industry, 2002. http://www.foresightvehicle.org.uk/info/_FV/init01_trm.pdf.

Roberto Saracco, Annaflavia Bianchi, Robert Dalla Mura, Graziella Spinelli, and Telecom Italia Lab. "Key European Technology Trajectories - First Report ." FISTERA, 2003.

Roberto Saracco, Edson Azevedo, and Telecom Italia Lab. "Key European Technology Trajectories - 2nd Report." FISTERA, 2004.

“ROCKET - Roadmap to Communicating Knowledge Essential for the Industrial Environment .” ROCKET, 2003.

“Scenarios and Solutions for the Future of Transcription .” American Association for Mediation Transcription and the American Health Information Management Association.

“Science and Technology Cluster: Overview of Key Trends up to 2015-2020.” Office of Science and Innovation, 2006.

“Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview.” European Commission, 2003. <http://www.it46.se/docs/articles/eur20823en.pdf>.

Sheridan Morris. “The Future of Netcrime Now: Part 1 - Threats and Challenges.” United Kingdom Home Office , 2004. <http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf>.

“Siemens - Pictures of the Future - Spring 2002.” Siemens , 2002. http://w1.siemens.com/innovation/pool/en/publikationen/publications_pof/pof_spring_2002/PoF_1-02_D_1203222.pdf.

“Siemens - Pictures of the Future - Spring 2004.” Siemens , 2004. http://w1.siemens.com/innovation/pool/en/publikationen/publications_pof/PoF_Spring_2004/PoF104art15_1194688.pdf.

“Siemens - Pictures of the Future - Spring 2005.” Siemens , 2005. http://w1.siemens.com/innovation/pool/en/publikationen/publications_pof/PoF_Spring_2005/PoF104art15_1264187.pdf.

Stephen Pullinger. “EU Research and Innovation Policy and the Future of the Common Security Policy.” ISIS Europe. ftp://ftp.cordis.europa.eu/pub/foresight/docs/ws7_csfp.pdf.

“Technology and You: Singapore Infocomm Foresight 2015.” Infocomm Development Authority of Singapore, 2005. http://www.ida.gov.sg/doc/Technology/Technology_Level1/20060417212727/ITR52005.pdf.

“Technology Foresight Pilot Project.” BioSystemics , 2003.

“The Future of Biometrics: Market Analysis, Segmentation, and Forecasts .” Acuity Market Intelligence, 2007. <http://www.acuity-mi.com/hdfsjosg/euyotjtub/execsumm.pdf?code=S01>.

“The Future of Health Care .” Parliament of Finland , 2006. <http://web.eduskunta.fi/dman/Document.phx?documentId=kb11307103133600&cmd=download>.

“The Future of Money .” OECD, 2002. <http://www.oecd.org/dataoecd/40/31/35391062.pdf>.

“The Future of Privacy; Volume 1 Private Life and Public Policy.” DEMOS, 1998.

Toni Ahlqvist, Henrik Carlsen, Jonas Iverson, and Ernst Kristiansen. “Nordic ICT Foresight.” VTT Technical Research Centre of Finland, 2007. <http://www.vtt.fi/inf/pdf/publications/2007/P653.pdf>.

“Turning the Corner.” Foresight, 2000.

Valerie Frissen, Jeremy Millard, Noor Huijboom, Jonas Svava Iverson, Linda Kool, Bas Kotterink, Marc van Lieshout, Mildo van Staden, and Patrick van der Duin. “The Future of eGovernment.” European Commission, 2007. <http://ftp.jrc.es/EURdoc/eur22897en.pdf>.

Wieslaw Bicz. “Future of Biometrics.” OPTTEL, 2006. <http://www.optel.pl/article/future%20of%20biometrics.pdf>.

Endnotes and Figure/Picture References

1. “Market Growth.” <http://www.covetek.com.au/Info/Info3.htm> (accessed 1 March 2009)
2. Data only; Roger, Allen (2008). “Figure-1: Biometrics Look to Solve Identity Crisis.” http://electronicdesign.com/files/29/19098/fig_01.gif (accessed 1 March 2009).
3. “Market Growth.” <http://www.covetek.com.au/Info/Info3.htm> (accessed 1 March 2009).
4. Ibid.

Future Issue Biometrics

The Uncertainty of Identification & Authentication: 2010-2020

June - 2009

Authors:

George Boone

Jonathan Huang

Stephan de Spiegeleire

Tim Sweijs

Artwork and Design:

Richard Podkolinski

George Boone

The Hague Centre for Strategic Studies (HCSS)

Lange Voorhout 16

2514 EE The Hague

The Netherlands

Telephone +31(70) 318 48 40

Telefax +31(70) 318 48 50

Email: info@hcss.nl

Website: <http://www.hcss.nl>

© 2009 The Hague Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/or published in any form by print, photo print, microfilm or any other means without previous written permission from the HCSS. All images are subject to the licenses of their respective owners. All information which is classified according to Dutch regulations shall be treated by the recipient in the same way as classified information of corresponding value in his own country. No part of this information will be disclosed to any third party. The views expressed by the author do not necessarily reflect the opinion of HCSS. If you have any comments on this document or any other suggestions, please email us at info@hcss.nl. All HCSS publications are available at the HCSS website: www.hcss.nl.

