Global terrorism is on the rise. For many years, the West felt immune to these incidents, often asserting that these were problems felt only in countries with heated conflicts, such as Syria, Iraq, Israel and Nigeria. However, recent terror attacks have taken place in both Europe and the United States: Belgium, France (Paris and Nice), Orlando, various cities in Germany, Turkey, and the list goes on.

The intelligence community is constantly looking for a single-point “source” to help prevent the next terror attack. However, in my experience serving as Head of Military Intelligence of the Israel Defence Forces, and through my work with the international intelligence community, I have learned that such a single source does not exist. There is no simple solution to terror prevention.
Proactive and combined approach

But taking a proactive approach can help the fight against terror. To be proactive, the intelligence community must create an ecosystem of information—a network of interconnected sensors that combine to provide a clearer picture of the situations that security agencies must assess to prevent attacks from happening.

*The intelligence community must create an ecosystem of information—a network of interconnected sensors that combine to provide a clearer picture.*

When it comes to preventing terror, this network might include an array of sensors: signal intelligence, cyber intelligence, visual intelligence—not only from satellites—surveillance balloons, drones, special forces, human intelligence, interrogations and others. Any of these sources alone would not get the job done; combined, however, they provided a clear picture of the security landscape.

Intelligence agencies collect all these single points of information and fuse them together. Almost in real-time, this fusion creates actionable intelligence for end-users (special forces, air force, any actor who can utilise the intelligence). This combining of sources we employed in my career led me to understand *the power of fusion.*

The power of fusion is the key to effective preventative security.

Global megatrends and demand for convenient security

There are two relevant megatrends in the world right now:
Urbanisation and the rise of the megacity, which inevitably leads to rising crime rates

The need to prevent terrorism

With these two relevant trends, increased security has become a necessity. However, there is a misconception that increased security means increased inconvenience for people. As such, there is a need to create systems that provide the high level of security necessary in today’s world, given the aforementioned megatrends, while still maintaining the convenience and pace in our everyday lives.

Biometric technology provides an answer to this. If we can quickly and securely identify individuals before they enter a building—or prevent them from doing so—many security crises can be prevented before they take place.

**Power of fusion and multi-modal biometrics**

This is where the power of fusion comes into play. Any biometric sensor on its own – facial recognition, fingerprints, iris recognition, voice recognition—cannot provide the accuracy, speed, or ease of use needed for strong security that is also convenient for the public.

Developing an effective biometric technology for secure access requires us to build a new intelligence ecosystem—a fusion of technologies that provide speed and accuracy, and are simple for the end-user. The most secure and convenient biometric technologies for identity verification must use the power of fusion. We find these types of solutions in multi-modal biometric technologies.
Multi-modal biometrics allow people to move freely, yet securely, through their daily lives

Multi-modal biometrics refers to a technology that combines a number of biometrics working together as a multifactor solution. This can include software that uses a fusion of biometric technologies, smartphones that require access via a fingerprint and PIN code, or access through voice and facial recognition, to name just a few. The primary advantages of such systems are the heightened levels of accuracy and security, as well as greater levels of accessibility and flexibility for users.

The industry is trending towards adoption of multi-modal biometrics. This is because stand-alone biometric technologies, such as iris scanning, face recognition, fingerprinting or otherwise, are exposed to a) questions of accuracy and b) the ability for fraud to attempt to trick the system.

But, by fusing a number of technologies such as face, body and voice, we can create a system that is highly accurate. In cases in which in-motion identification is part of the technology, a user may not even be required to stop for identification. This fusion of sensors allows us to identify a person in real-time, with high accuracy and speed. By employing the power of fusion, neither security nor convenience need be compromised.

Adoption and real world use of multi-modal biometrics
The use of multi-modal biometrics is expanding, and is being sought after by some of the largest companies in the world to secure facilities. Market research firm Technavio predicts that the global advanced authentication market (multi-factor and biometrics solutions) will experience a CAGR of 17 percent between 2016 and 2020. Lead analyst Amrita Choudhury commented that threats in the realm of digital security in retail, healthcare and the banking and financial services industry are driving companies toward multi-modal biometrics. According to Choudhury, multi-modal biometrics will likely gain widespread acceptance over the next four years.

The use of multi-modal biometrics is expanding, and is being sought after by some of the largest companies in the world to secure facilities.

While we often see multi-modal biometrics in homeland security, military and law enforcement applications, more often, these technologies are being deployed for consumers. For example, certain smartphones, such as the Samsung Galaxy 5S, utilise face and voice biometrics for greater authentication accuracy. We can also see these technologies in banking apps and cloud platforms focused on the enterprise security market.

However, multi-modal biometrics are certainly not limited to the digital/cyber realm. In fact, physical locations – buildings, healthcare facilities, corporations, schools and universities, stadiums and airports could all benefit from more secure and more convenient access made possible by multi-modal biometrics.

We live in a world in which we contend with new threats created by rising crime and terror. By applying the power of fusion to physical secure access technologies, we can increase the level of security that is necessary without feeling that we live in a police state. Multi-modal biometrics allow people to move freely, yet securely, through their daily lives, providing access to those we
recognise, and allowing the power of fusion to prevent access to those who are unfamiliar. In this way, we can practice proactive preventative security without encroaching on the pace of life.

Author Profile

Aharon Zeevi Farkash
Biometrics’ greater convenience and cost-effectiveness expands its application...

The universe of biometric authentication applications is expanding rapidly in vertical markets such as healthcare and retail...

Biometric authentication offers greater security advantages over traditional methods...

Accurately confirming a person’s identity is one key to improving security for our workplaces, communities, and our nation...

Biometrics prove best for preventing time & attendance fraud...

Time and attendance has proven to be a successful use of biometric technology traditionally used for controlling access to high-risk areas...