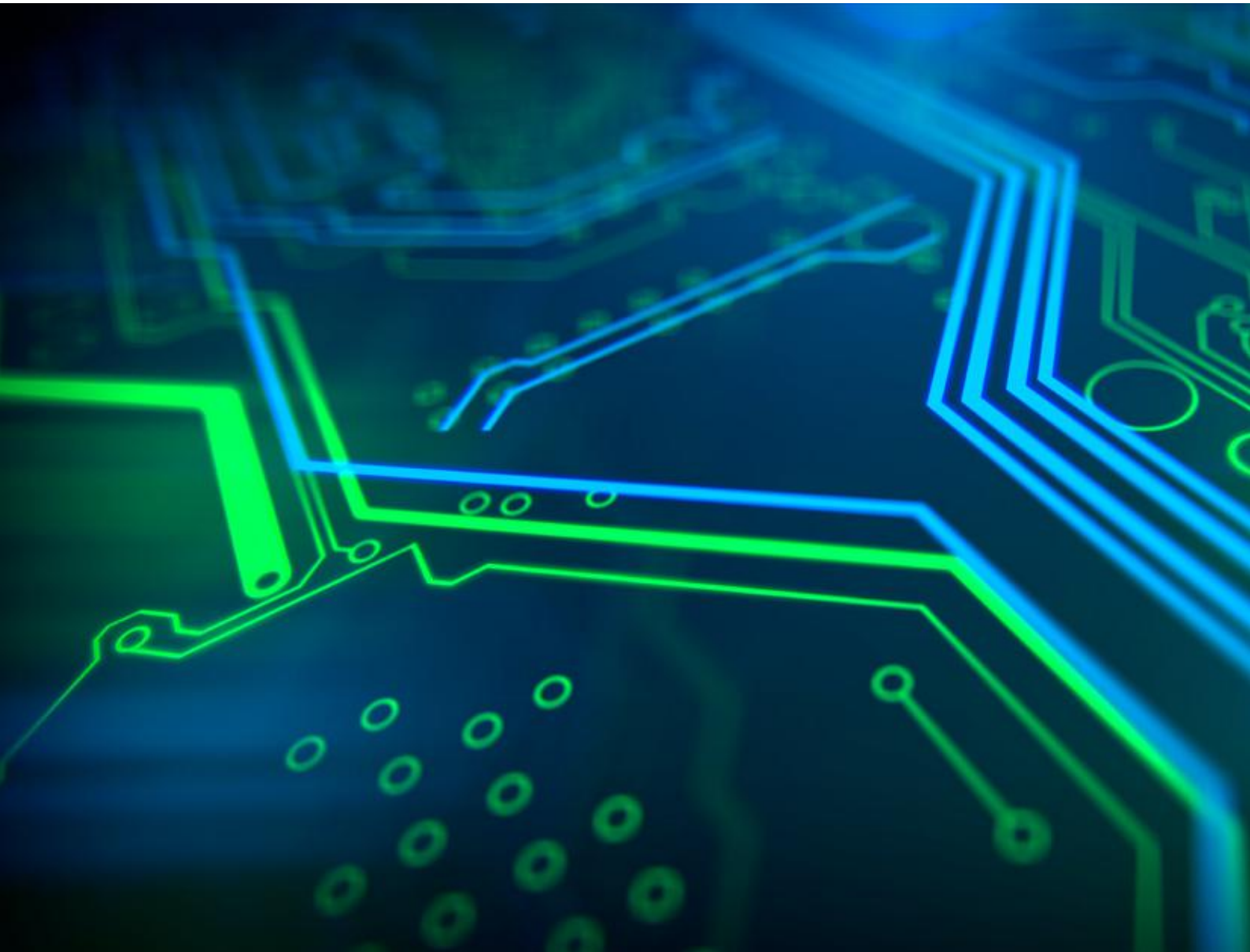
IHS Markit®

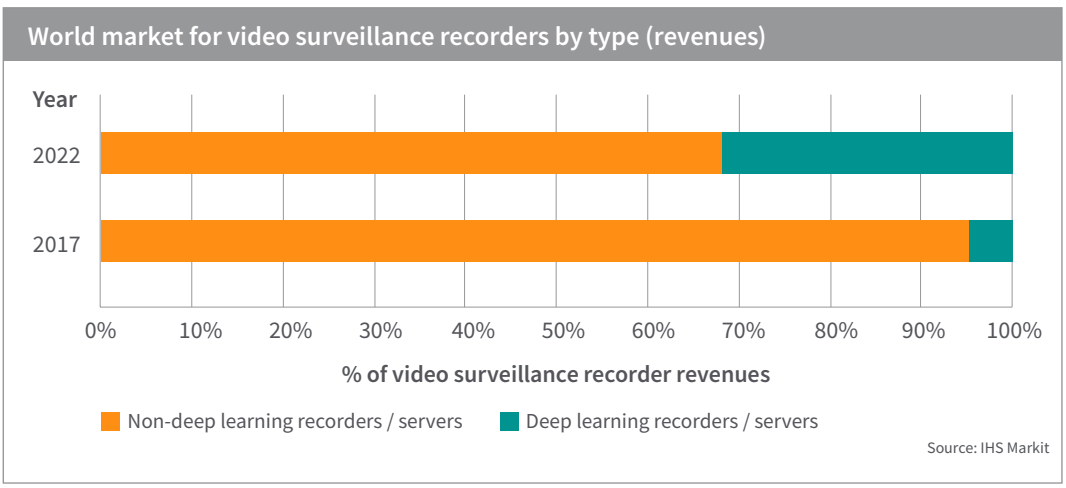
Artificial Intelligence in Physical Security

An overview of market and technology opportunities



Artificial intelligence (AI) is the body of science, algorithms, and machines that are able to perform some version of learning and independent problem solving, based on advanced software and hardware components. Data is also core to AI; large datasets are the foundation for recent performance improvements across market applications. Within the AI field of study are other sub-branches of computer science, including machine learning, neural networks, and deep learning.

The speed of development in AI has aided its adoption in several industries—including smartphones, healthcare, and automotive. Likewise, the physical security market is increasingly looking to adopt artificial intelligence applications, in particular in the case of deep learning algorithms in the video surveillance market. In fact, the deep learning enabled recorder market is forecast to account for over 30 percent of total video surveillance recorder market revenues by 2022.



AI is currently implemented on devices, in the cloud, or a hybrid combination of both approaches. Each approach comes with its own unique set of advantages and disadvantages. For example, cloud AI has more computing power to analyze data and run powerful deep learning algorithms, but there are potential issues around privacy and latency.

A stronger on-device AI would help offset these dangers to some degree. However, compute power and integration potential become more of a challenge for the AI application. It is likely that the physical security industry will develop a variety of deployment topologies, with dedicated servers deployed first followed by cloud and potentially on-camera analytics if the processing power requirements can be met.

This white paper aims to provide an introduction to artificial intelligence and how it could be applied to the physical security market. Examples of real deployments are discussed as are potential market opportunities to highlight how the industry will evolve as artificial intelligence becomes a more prominent technology.

Machine learning, ANN and deep learning

Since the 1980s, academics have worked on the concept of AI machine learning, which has often been associated with artificial neural networks (ANN) and, more recently, deep learning architectures. Deep learning is a way to emulate the functions of the human brain, using electronics and software algorithms.

A system relying on neural networks differs from conventional pattern-recognition systems, in that it will continuously learn from experience, and base its ability to discern and recognize its surroundings like human beings do: by learning from real sounds, images, and other sensory input.

Although ANN and deep learning are not new concepts, a deep learning breakthrough occurred in 2015, which abruptly reduced the machine vision error rate. During a machine-vision competition, ImageNet - a large visual database designed for use in visual object recognition

software research - succeeded for the first time in surpassing the five percent average human error rate, when analyzing a database of images.

Such a rapid enhancement was caused not only by progress in advanced algorithms, but also by the development of new and much faster hardware systems based on massive parallelism on graphics processing unit (GPU) cores, instead of traditional central processing units (CPUs). These new architectures allowed faster learning phases, as well as more accurate results, principally because GPUs can train neural network models 100 times faster than a CPU.

AI in video surveillance

Advancements in the use of artificial intelligence based technologies in video surveillance has accelerated in recent years. This is despite the industry being relatively slow to adopt new technology: the consumer TV market is already looking to 8k resolution and has a third of all shipments at 4K resolution or above while 4k security cameras (and above) accounted for only two percent of all network camera shipments globally in 2017.

As the number of cameras installed increases year on year, so too has the amount of video images that are generated. In order to use this video efficiently, the market has looked to deep learning, the same technology that is enabling autonomous cars and helping doctors use computer assisted diagnosis for scans. In the last couple of years, there has been a marked increase in research and development in deep learning neural networks, proving their capabilities, generating considerable excitement, and putting them within reach of a much wider user group.

For years, the reliability of video analytics has been extremely variable, with vendors struggling to develop algorithms that could function in complex scenes. And whilst the capabilities of rules based video analytics have steadily increased, they are not quite able to provide the insight and accuracy that is needed.

Deep learning neural networks are able to offer a level of accuracy and reliability in object and behavior detection and classification significantly greater than traditional rules based analytics. Broadly speaking, there are two main areas in which deep learning analytics offer benefits over the technology that has preceded it.

Accuracy

A long-held complaint levied against traditional rules based analytics products was that their algorithms were unable to distinguish between objects and behaviors that a human being would have no problem classifying. This is due to traditional algorithms being based on geometric rules. This weakness in human designed computer vision algorithms results either in missed security breaches or false alarms.

The ability of deep learning algorithms to view a scene intuitively, as a human viewer would, means that detection accuracy increases dramatically. Neural networks allow a computer to apply a series of assessments to a given situation learning to identify increasingly more sophisticated features (edges, colors, shapes and tones), unlike rules-based solutions which are limited to the initial programming. Also, as compute power continues to increase, neural networks will leverage this to process more data and improve accuracy. This is an important development for the video analytics industry.

Power

Deep learning has demonstrated its capacity to increase the effectiveness of a computer to reliably classify objects and behavior. It is also improving the processing and analysis of increasing volumes of video footage. A combination of more powerful GPUs, and the ability for analytics to automatically detect, recognize, and classify objects has made video searchable. Companies are now marketing analytics that can leverage deep learning to turn vast amounts of video footage into usable information in a fraction of the time it would have taken in the past.

Video processing software also allows users to interact with the surveillance footage using a Google-like interface with natural language search terms such as “FedEx van”, or “delivery man on driveway”. This makes the video search easier to use and drastically reduces the time it takes to find relevant footage in an archive that might store video from thousands of cameras.

In addition to this, the ability to detect multiple objects and classify them allows for much greater insight to be gained from the video. This extends the ability to recognizing a cars color, type, make, model, and analyzing which direction and speed it is moving at, making it possible to draw patterns, insights and conclusions based on the data.

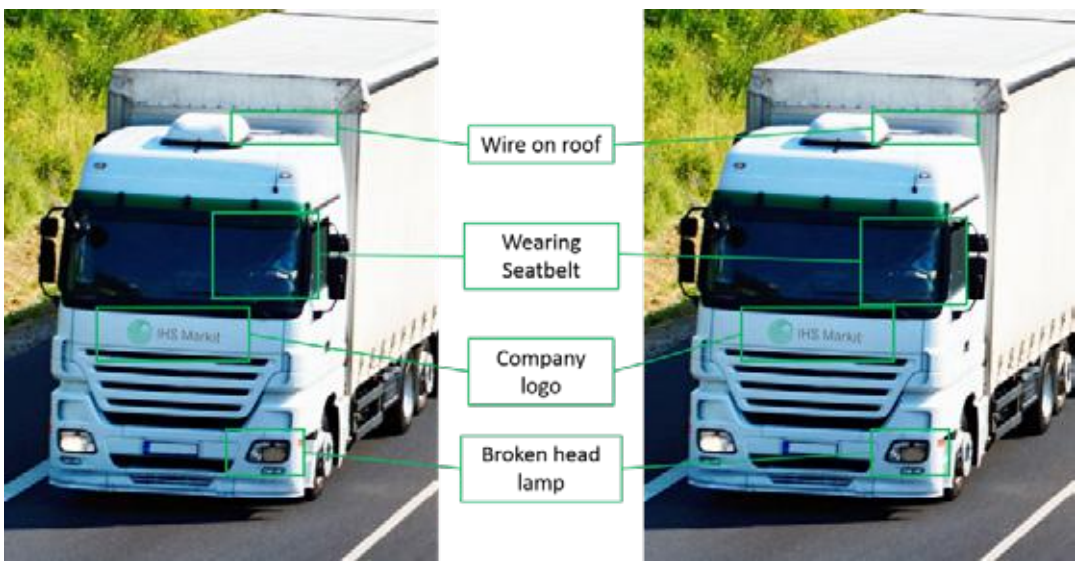
Traffic Management

Increasingly safe city projects are being deployed in conjunction with traffic monitoring and traffic management solutions.

A single camera offers only limited insight into a city’s traffic, so these solutions tend to be large, typically in the thousands of cameras. This requires a more comprehensive analytic tool to analyze all of the data that is collected from the cameras. The only feasible approach is to use deep learning analytics to assess individual camera images for ANPR (Automatic Number Plate Recognition), vehicle recognition, and pattern analysis across multiple cameras.

One of the many benefits of deep learning analytics is their ability to more accuracy detect and recognize images. Solutions can also go one step deeper recognizing that a license plate and vehicle do not match based on classifying the car and checking against the country’s register of automobiles.

Some companies are also developing unique feature matching analytics. These analytics are able to take single images of a vehicle, and search across a city surveillance network based on a unique feature, such as stickers in the widow, a broken head lamp, dented body work, or items hanging from the rear view mirror. This can make searching for a vehicle used in a crime more efficient.



Due to the improving accuracy of object recognition algorithms, deep learning analytics are also being used for driving offenses, and can detect if a driver is on their cell phone or not wearing their seatbelt.

Face recognition

Most facial recognition analytics on the market today feature some kind of deep learning. Not only does it increase the accuracy of facial recognition sensors, it also enables faces to be identified in larger and more crowded scenes. In the wake of recent terrorist attacks in crowded locations, this capability could change the whole approach to security monitoring, allowing law enforcement to track suspects with greater speed and efficiency.

However, deep learning analytics are doing more than just improving accuracy rates. They are also enabling the system to make assumptions and provide business intelligence on a detected face. Age and sex recognition algorithms, which are particularly popular within retail applications, allow end-users to profile potential customers and target marketing material appropriately. Furthermore, some vendors claim to be able to recognize a person's emotions through analytic algorithms. There remains some debate as to the accuracy of these solutions currently.

One area where facial recognition has the potential to disrupt, is in the access control market. Facial recognition solutions have been used for a number of years at passport control in airports. However, as the price of the technology and cameras reduces, it is expected that facial recognition will be used to prevent access to restricted areas. Some of the benefits would include:

- Lower operational costs: whilst the initial outlay for the analytics and additional cameras would be more expensive, there would be no card replacement fees. This can run into the millions of dollars per year in some installations, such as airports.
- Access is more secure: access cards can be handed to other people to use, facial recognition prevents this. In addition, it also prevents doors being held open by a valid access card to allow other people to walk through.

There are also a number of challenges with using facial recognition for access control:

- Enterprises and governments require employees to wear badges anyway for identification purposes. This reduces the cost benefits.
- A camera is required on all the doors with electronic access. Depending on the size of the installation this could be thousands of cameras.
- Card readers have a life expectancy of up to 20 years, so it could be a long wait before the installed base is ready to invest to replace them.

AI in Access Control

Risk-Based Access Control

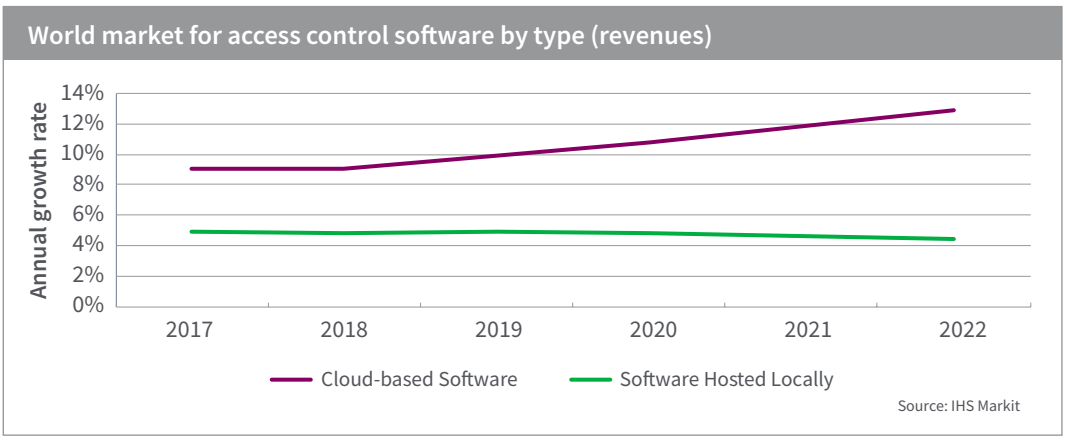
In nearly all access control systems, the authentication process is a singular event; a credential is presented and access is granted or denied. However, by leveraging the advanced capabilities of neural networks this process can be made more intelligent.

At a basic level, risk based access control can be summarized as follows: in many sports stadiums public office space is combined with the actual sports stadium. Access to the office locations needs to be open when workers are accessing it during the week. However, when the sports event is on this access should be restricted and only provided to key personnel with the correct access control credentials.

In the example given the authentication process is dynamic, depending on circumstances. This allows the system to shift gears and provide a higher level of building security when certain events happen.

By introducing the intelligence of AI to a risk-based access control authentication decision, the process can be made more complicated. Instead of defining risk levels by looking at the events currently on in the building, the system could pull data from other security or building management systems or social media alerts to make decisions based on this data.

The main barrier to developing this level of complexity using traditional rules-based analytics is that there are simply too many variables to account for. The use of neural networks means developers do not need to write rules for the system to follow, they simply need to provide the algorithm with objectives and training data. Over time, the system will be able to decide how all of the inputs should relate to the current risk level.



Access control software hosted in the cloud is on the rise (see chart).

The level of processing power needed to conduct AI analytics will likely benefit from cloud architecture. Companies are already looking to move their servers offsite and it is very unlikely that they would want to purchase (even more expensive) servers to host AI software on site.

Furthermore, cloud-based access control software is often easier to integrate with other building management software. It is also easier to keep up to date and ensure everyone is running the same version of the software. This lowers the cyber risk.

AI in other Physical Security

Alarm monitoring verification

Artificial intelligence has the potential to improve the alarm monitoring market. When alarm events occur, central stations follow a number of routes to try to verify the alarm. These include calling the home owner, attempting to verify the alert through a series of video images, and direct dispatch.

AI could help to automate this process providing a pre-assessment of the alert based on data analysis. In the future audio recognition and face recognition could be deployed to support the operator in their assessment of the incident. Reducing the cost of false alarms and responding quicker to real events would be of great benefit to the industry. AI could also support integration between self-monitoring and professional monitoring, making smart decisions on when a professional service is required. AI voice assistants might even replace human operators, although this is likely a long way in the future.

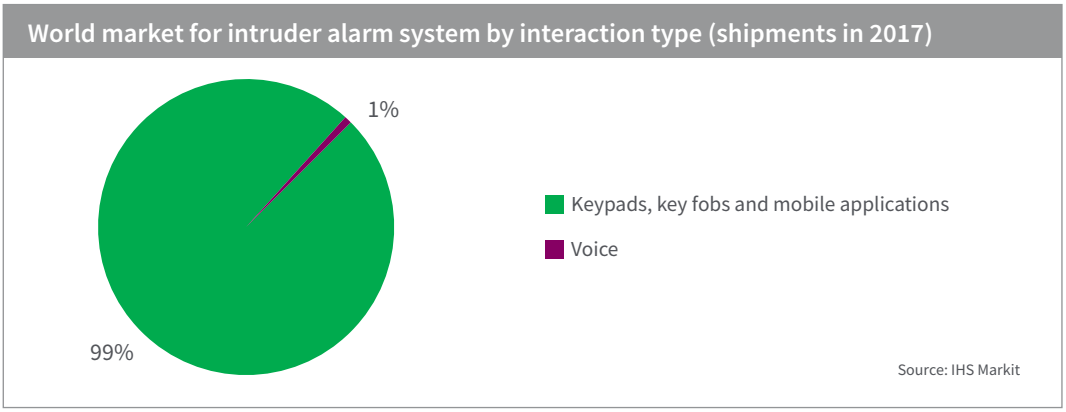
Alarm arming and disarming

Smart speakers like the Amazon Echo and Google Home have introduced a form of AI into the home security sphere by allowing digital assistants to arm and disarm the intruder alarm system.

When arming the system, the user can now just ask the voice recognition system. Disarming the system typically needs some form of code or a password for additional security. Future iterations of this solution may be able to recognize the user's voice or integrate with other sensors, such as face recognition, to more fully automate the process and make it more secure.

Furthermore, if the various inputs - voice, image, and motion sensor data to name a few – can work in harmony, the system could reliably detect whether movement in the home is an intruder or the home owner who is allowed to be there.

This is the premise of a true smart intruder alarm system; however, with current voice integration at one percent of total systems in 2017 there remains a long way to go before this solution is ubiquitous in this market application.



Real-time crime centres

Predictive analysis tools have come a long way since the first products and solutions. Police agencies can now make use of a wide range of data inputs and advanced data mining techniques to predict where criminal activity is likely to occur. This approach is called the predictive crime center and it is becoming an important part of modern policing.

Data from video surveillance, traffic management cameras, audio analytics, gunshot detection, weather systems, and other public safety systems are analyzed in parallel to identify patterns and potential threat events. Over the past few years, social media has also become a viable tool in public safety. In many cases, incidents are first reported on social media platforms such as Twitter and Facebook. Analyzing the data "hose" is challenging but can support quicker emergency response times when applied successfully.

The future predictive command center will be reliant on powerful analytics software to extract intelligence from the unstructured data sources routed into command centers. The solution must be open to ensure that enough data is fed into the big data solution. Artificial Intelligence will play a key role in navigating this data, recognizing patterns and making intelligent decisions independently of the human operators.

Related, a more localized solution to predictive alerts could be implemented in the suburban environment. AI could be used to identify criminal behavior such as burglary and theft. Deep learning video surveillance cameras could support the process, alerting to triggers such as loitering, repeatedly walking past the same spot and wearing clothing that makes it hard to identify an individual. Artificial intelligence in this case could also make better use of the crime data available – in terms of frequency, time, approach, and direction, to more accurately predict future criminal events.

Finally, in the residential market, this type of sensor fusion of face recognition, behavior recognition and data analysis could provide new solutions protecting from kidnappings, burglary and assault in the home.

Market challenges and growth drivers

Algorithm efficiency

In the video surveillance analytics market, some algorithm developers are using AI in the form of deep learning to maximize their output efficiency. These independent software vendors (ISV) are training the algorithm mostly in the cloud, using solutions such as AWS (Amazon Web Services). Heavy compute power is expensive so it is leased.

Deep learning is primarily being used to develop and improve the algorithm quickly. This acts as an equalizer when compared with the large, multi-national suppliers. In the past, a team of coders were required to develop analytics. The speed and quality of the analytic was directly

impacted by the team's size. Now, analytics can be developed for niche applications quickly and with much less resource meaning boutique analytics houses can compete. Furthermore, most of the large suppliers are focused on one-size fits all algorithms, leaving opportunity in niche applications.

China

China has shown a clear commitment to develop and invest in AI technologies. The blueprint released recently by the Chinese state council, to position China as a leader in the development and deployment of artificial intelligence technologies, shows a roadmap with milestones in 2020, 2025 and 2030. China has several advantages over other countries, including the following:

- A large population of software developers coding AI projects.
- Huge amount of gathered data.
- Easier process for making new laws and regulations.
- Generous government funding programs.

The Chinese community has also recognized the strategic role semiconductors play in the overall economy. There has been a strong push to support strategic silicon providers which are entirely focused on AI. This all positions China strongly in the future roll-out of AI technology in the physical security market.

China has been a leading adopter of deep learning analytics in the video surveillance market. Many of its safe city and city surveillance projects specifically require deep learning to be deployed which has driven research and development in this technology.

In addition to deep learning vehicle recognition and traffic monitoring analytics, 2017 saw an increase in the deployment of deep learning facial recognition analytics in China's safe city projects. It is now regularly specified in tender documents, signaling that the shift toward deep learning-based video analytics is well underway.

Deep-learning analytics continue to generate more metadata than in the past. In light of this, cloud architectures are being adopted to enable data sharing more easily and across much larger and more complex networks. The adoption of cloud and AI are key technology trends and growth drivers in China, the world's largest video surveillance market.

Brand

Although AI will certainly add value and new functionality, in the short term it will also be a brand differentiator. In the same way that companies released high megapixel video surveillance cameras to show what was possible, AI demonstrations will provide an insight into the future of the physical security market.

AI will also enable new business models and new players to disrupt the market. In the future, it will be extremely important for service, functionality, efficiency and profitability, as well as for companies to remain relevant and survive in the physical security market. One challenge that the market will have is how to productize the application of deep learning analytics. Companies that tell this story well will be successful. The other challenge will be timing; technological challenges, market acceptance, and high costs mean it could be difficult to make money from AI in the immediate market environment.

Channel investment

AI is a new technology and as such it requires investment from all participants in the physical security market in order to succeed. The real world impact of Artificial Intelligence technology on physical security companies will depend on their position in the channel and, to a lesser degree, who their customers are.

Video surveillance is at the bleeding edge of AI deployments in the industry. Consequently, in the short-term, video surveillance equipment manufacturers will be most impacted by the AI

evolution. In the same way that growth in the network video surveillance market has reduced the total market opportunity for analog suppliers, AI is forecast to gain share meaning vendors not supplying the technology will be competing for a smaller piece of the revenue pie. That being said, the pace at which this transition happens remains up for discussion.

Access control, intruder alarm and other peripheral manufacturers will have longer to prepare their AI strategy. For these companies, open partnerships and education are important activities, but deploying AI on the equipment is likely cost and technology prohibitive at this time.

Systems integrators with strong video surveillance portfolios and a focus on enterprise-level customers will also need to educate their business in AI. However, integrators in the mid-market will have longer to prepare as the initial cost of deep learning will limit penetration in the smaller commercial projects.

Central monitoring stations will also have longer to prepare for the impact of AI. In the immediate market, only very high-end enterprise video monitoring solutions are likely to use deep learning technology. In the future, deep learning technology could impact everything from alarm verification (video analytics) to alarm response (AI operators). Although this technology application is likely decades from market readiness, it does pose a significant threat to the current business models employed by these service providers.

There is also an element of belief required. The technology is still developing and some of the marketing does not accurately describe the benefits of today's AI solutions. At some point in the future this will change and AI will deliver on much of its current promise. When this happens, those that have not engaged with the technology will very likely be left behind, just as those that stayed with analog video surveillance were left behind.

Data

AI supports more detailed statistical analysis of the operations of security departments. However, one of the challenges for "big data" is in having enough data to make reliable statistical conclusions. As we have already highlighted, the short-term data analysis opportunities will likely be in situations where large data sets are created such as in safe city projects. Smaller companies may not be able to make accurate decisions based on a more limited data set. Ultimately, AI is required to identify that thing that does not belong in the data: this requires enough data to recognize anomalies, not just new content.

Another challenge is in normalizing the data. Social media represents an important new source, but in order to alert to abnormal behavior there needs to be an assessment of what is normal behavior. Consequently, normalizing the data set is critical to assess what is the typical amount of conversation around a specific topic.

Chat bots

The physical security market could also learn from other industries in applying AI to customer service. Natural language processing is improving and chat bots are increasingly used by consumer facing companies to provide an artificial intelligence interface for their users. This type of technology could be deployed to support physical security and employee security applications in the future.

Cyber security and data risk

As discussed, the performance of an artificial intelligence algorithm is linked to the quality and size of the available dataset. In an increasingly connected world, new physical security sensors are being deployed all the time, driving different data types into the AI solution. While this is great for the evolution of deep learning algorithms, it does present a threat in terms of cybersecurity.

Historically, the biggest challenge for cybersecurity in the physical security market has been the lack of awareness throughout the route-to-market. End-users often underestimated the force of cyber threats and integrators and equipment suppliers were not focused on building cyber protection into their solutions.

More recently, equipment vendors in the video surveillance and access control markets have shown more commitment towards cyber security. Responses have included product hardening guides, encryption certification, the auditing of firmware code and partnerships with dedicated cyber security solution providers.

However, many of the connected device start-ups entering the physical security market don't have the resources to focus on cyber security and will remain a threat to the overall solution. As the large IT companies improve their cyber defenses, it is likely that attacks on IoT vendors will increase in regularity and intensity. Ultimately, these companies will provide an easier target to hackers looking to maximize their impact.

AI is also relevant in terms of cyber security technology. For example, the defense market is already using deep learning applications to analyze cyber data to better protect critical national infrastructure. Many industry observers think that hackers will use this technology to escalate their attacks in the future too, increasing the cyber threat further. There are also some concerns related to how AI solutions interpret inputs and whether this could be manipulated by cyber criminals to cause confusion and damage in the future.

Related to the cyber threat, data privacy and risk will also be important considerations as AI solutions become more pervasive. Data encryption of video surveillance images is not common at the moment; mostly it is used in healthcare or critical infrastructure. GDPR (General Data Protection Regulation) in the EU could define video as unique personal data which may change the encryption requirements for video feeds.

GDPR could also impact what data is stored and how it is shared, impacting the analytics market. In particular, face recognition and person classification analytics will be considered personal data and have constraints on what can be done with the information. In response, Belgium announced that it will be banning the use of facial recognition for private use. The legislation does allow access control law enforcement applications but is an example of how data privacy could impact the physical security AI market.

Lessons from other AI applications

There are lessons and opportunities for the physical security market in other industry segments. At its most basic level, autonomous cars trained with deep learning will be able to detect other cars that are driving, objects in their way, or people on the street. The self-driving car approaching an intersection will yield to pedestrians, but will also know when to engage in more "aggressive" behavior—such as in a four-way stop when it signals intent to drive through.

More AI-based systems are expected in infotainment, specifically in HMI (Human Machine Interface) applications in the future, including speech recognition, handwriting and gesture recognition, virtual assistance and a natural-language interface.

New mobility and the healthcare industry are already taking advantage of AI, but industrial automation and manufacturing, robotics, energy and utilities, smart cities, and banking and financial sectors can also benefit. The direct and indirect effects of AI on these business sectors will be massive, especially how it affects product offerings (e.g., services and applications), AI smart-industry automation, AI-based augmented processes and interfaces, and manufacturing efficiency, productivity and costs. AI could spur 20 percent to 40 percent growth in these industry segments over the next 15 years, beyond what would be expected without AI.

In consumer electronics, "Alexa-ready" functionality is driving the adoption of microphones in consumer electronics, appliances and smart home devices. The smart speaker market on its own is forecast to grow to 85 million units shipped in 2021.

The ecobee4 thermostat has a microphone embedded in the device to offer voice assistant functionality without the need for a smart speaker. This trend is likely to continue. IHS Markit estimates that 60 percent of all smart home devices will be either integrated or embedded with voice control/assistants by 2021.

While the Alexa solution does not overtly promote the retail business in most applications, the capability is there and the belief is that consumers will increasingly be comfortable with ordering products and services with voice only. We are already seeing these types of applications with voice ordering of both Uber taxis and take-away pizza. Furthermore, recent studies have shown that voice assistants are driving an increase in on-line sales.

One thing is clear: AI will cause profits to grow in a wide range of applications. How the advantage in profitability will be used, in terms of the human work force, is a major concern, which will eventually require the work of regulatory bodies to figure out. This will impact the physical security industry as much as any other end-user application and will be an important consideration in the future.

AI is the future – and it's here now

AI will be disruptive to many industries – not just the physical security market. Moreover, the impact of AI will not be just on industries and finance, but our entire society, especially in the areas of privacy and data security, labor, and ethics. The need for data security and privacy is more essential today than ever, given the availability of such powerful technologies.

The physical security market is primed to benefit from AI for two reasons:

- AI, in the form of deep learning algorithms, has the potential to revolutionize the video surveillance analytics market providing face recognition, object recognition and behavior recognition at a reliability level that will really matter to end-users.
- The physical security industry generates data. Video surveillance images, access control data, audio analytics, social media, police records management systems and other IoT sensors all generate data that can be correlated and analyzed by artificial intelligence systems to build a safer society. Intelligently managing this data is huge challenge. AI can help solve this problem.

The challenge for physical security vendors, end-users, and integrators will be how to make the most of the AI opportunity. This will involve investment, education and judgement to best apply this transformative technology to the individual challenges faced by each participant.

For more information www.ihsmarkit.com

CUSTOMER CARE AMERICAS
T +1 800 447 2273
+1 303 858 6187 (Outside US/Canada)

CUSTOMER CARE EUROPE, MIDDLE EAST, AFRICA
T +44 1344 328 300

CUSTOMER CARE ASIA PACIFIC
T +604 291 3600

E CustomerCare@ihsmarkit.com

About IHS Markit

IHS Markit (Nasdaq: INFO) is a world leader in critical information, analytics and solutions for the major industries and markets that drive economies worldwide. The company delivers next-generation information, analytics and solutions to customers in business, finance and government, improving their operational efficiency and providing deep insights that lead to well-informed, confident decisions. IHS Markit has more than 50,000 key business and government customers, including 85 percent of the Fortune Global 500 and the world's leading financial institutions. Headquartered in London, IHS Markit is committed to sustainable, profitable growth.

274946964-CU-0918