Top Video Surveillance Trends For 2018

By the IHS Markit
video surveillance group

Introduction

Demand for professional video surveillance cameras has been growing quickly and is forecast to continue growing in 2018. It is estimated that less than 10 million surveillance cameras were shipped globally in 2006. This grew to over 100 million in 2016. It is forecast that over 130 million will be shipped in 2018.

Despite this increase in demand, the average price of cameras and other video surveillance equipment will continue to fall quickly. As a result, IHS Markit is forecasting that in terms of US dollar revenues the world market for video surveillance equipment will grow at an annual rate of less than 6% in 2018.

It will be challenging for vendors to continue to grow revenues and margins, but there will be opportunities for well-placed vendors. For example, the South East Asian and Indian markets are both forecast to grow at higher than average rates. There is also great potential for the next generation of products powered by technologies like deep learning and cloud computing.

So, what will be the big stories in 2018? Deep learning, GDPR compliance and drone detection technologies are just some of the trends discussed in our eighth annual trends white paper. The following articles are designed to provide some guidance on the top trends for 2018 in the video surveillance industry. We hope you find them useful in planning for the year ahead:

- The A to I of video surveillance terminology
- The evolution of deep learning in video surveillance
- GDPR
- Big differences between the Chinese market and the rest of the world
- Drone detection technologies
- Video surveillance fault tolerance
- Forensic video analytics as a service
- Xue Liang program, a boost to the Chinese market

If you would like to speak with one of our analysts on any of the topics covered in this white paper, or to discuss our video surveillance service offering, please contact us.

Best regards

Jon Cropley

Senior Principal Analyst – Video Surveillance

For more information on this white paper, refer to the Video Surveillance research area, under the Security Technology section of the IHS Technology website.

Contact Information:

Americas: Technology_us@ihs.com

EMEA: Technology_emea@ihs.com

APAC: Technology_apac@ihs.com

The A to I of video surveillance terminology

By Jon Cropley

The past 12 months has seen a range of new terms becoming regularly used in the video surveillance industry. Below, we attempt to provide a brief summary of some of these. Please accept our apologies in advance for any oversimplification this attempt at brevity causes.

AI (artificial intelligence) - computers being able to perform specific tasks as well as or better than human intelligence. In the context of video surveillance, AI is used in the field of computer vision to classify visual images and patterns within them.

Big data – huge amounts of different information being stored, organized and analyzed by computers to identify trends, patterns, and relationships. In the context of video surveillance, the data could be metadata describing hours of video surveillance footage combined with other data sources to highlight patterns relating to security or business operations.

Cloud computing – instead of using a local server to store or manage video surveillance data, using a network of internet-connected remote servers. Generally this network has the ability to provide additional resource if and when required from a larger available pool. The available resource may be clustered into a datacenter or network of datacenters. These may be private (entirely or partly owned for exclusive use by specific organization/s) or public (resource accessible to multiple separate users).

Deep learning – a branch of machine learning and subset in the field of AI. Deep learning makes use of algorithms to structure high-level abstractions in data by processing multiple layers of information, emulating the workings of a human brain (a neural network).

Edge computing/storage - performing data processing and analytics/storage closest to the source of the data (normally, in this context, in a video surveillance camera).

Face recognition – when a video surveillance system can automatically match a person's face against a database of individuals.

GPU (graphics processing unit) - A programmable chip specialized for use in image processing. Due to the requirement to be able to simultaneously processing multiple large data blocks required in modern image processing GPUs have been found to be highly suitable for deep learning/neural network processing.

H.265 – (or MPEG-4 part 2) is a video compression codec standard approved by the International Telecommunications Union (ITU-T). Compared with H.264, H.265 has the potential to use 30–40% less bandwidth for a video stream of the same quality.

IoT (the Internet of things) – IoT is not a specific device or technology – it is a conceptual framework, driven by the idea of embedding connectivity and intelligence in a wide range of devices. IHS Markit defines an IoT device as a device which has some form of embedded connectivity that allows the device to be directly connected to the internet (i.e. IP addressable), or allows the device to connect (tether) to an IP addressable device. In the context of video surveillance, this could be using video surveillance data with other sensors or sources of information.

The evolution of deep learning in video surveillance

By Monica Wang

In last year's edition of our annual trends white paper, "Top Video Surveillance Trends for 2017", it was discussed that the biggest challenge for mass adoption of deep learning was the ability to demonstrate a security or business intelligence benefit to using the technology in the many different surveillance scenarios. 2017 witnessed great progress in the market with a transition from proof of concept deep learning algorithms to video surveillance products and a whole range of new entrants in AI chipset offerings. With the technology's concept more proven, future success will depend on the ability to demonstrate a return on investment from deployments.

Driven by the R&D investment from chip vendors, software startups and major video surveillance vendors, deep learning video analytic algorithms have been developed into fully deployable products with user-friendly interfaces and scenario-focused solutions. For example, deep learning face recognition algorithms are now available in search engine type applications, designed to find missing people from video footage.

Transitions such as these are evident in the Chinese market and in the products shown at the recent China Public Security Expo (CPSE) 2017. Full deep learning products on display were either software-based applications with deep learning or video surveillance hardware with embedded algorithms. As an increasing number of vendors develop deep learning algorithms, several software startups have also developed their own deep learning video surveillance hardware to cement their place in the market.

Transformation in deep learning cameras

Following the transition from analog to network cameras, the next stage will likely be a mass market transformation to deep learning enabled cameras. During the transition to network cameras, growth in shipments was accelerated due to large price declines. The worldwide average price of network cameras in 2016 was around one quarter of the 2010 level. A similar trend of large price decline catalyzing a rapid increase in unit shipments can also be expected for the future generations of deep learning enabled cameras.

So far, most of the deep learning cameras sold have been for safe city projects run by police departments in China. These projects are less price sensitive than the remainder of the market, where the average price is still too high for end-users. The cost of semiconductors which enable the deep learning algorithms to run in the cameras are a major component of camera prices. Following the release of deep learning cameras with Nvidia and Movidius chip solutions at CPSE 2016, more semiconductor vendors (including some from the mobile device market) also exhibited at CPSE 2017, highlighting their ambitions for the video surveillance market. Some of these vendors include XILINX, DeepHi Tech, Intel, Vimicro and Qualcomm. These new chip vendors entering this market are increasing the number of options available for the deep learning ecosystem and importantly are increasing pricing pressure at the chip level. This will enable a rapid reduction in the average price of deep learning cameras.

Outlook

Deep learning and AI are now more established buzz words, particularly in China, and the education of the market regarding the technology continues to increase. End-users are becoming more familiar with real world product deployments rather than just prototype demonstrations of an algorithm. Chinese vendors have begun to promote their deep learning products to the rest of the world. 2018 is set to continue this trend with increased sales from the Chinese vendors outside the Chinese market and more case studies from installations outside China.

The year ahead will also see greater differentiation of video analytics products based on an increased number of semiconductor vendors' chipsets. Besides the initial projects in city surveillance and transportation, more installations in retail and commercial buildings are likely to be the next to embrace the greater use of deep learning technology. As we've seen in the wider video surveillance market, a targeted vertical approach is likely to be a common strategy. Vendors that market vertically-focused deep learning applications aligned with their own existing portfolios should have good opportunities to grow.

GDPR

By Josh Woodhouse

In 2018 there will be an increase in the wider discussion about privacy and how the video surveillance industry protects the data it gathers. Much of this will stem from the new EU General Data Protection Regulation (GDPR) which will become law across EU member states (including the UK) in May 2018. However, the effects of GDPR and compliance will also have far reaching implications outside the video surveillance industry.

GDPR will replace each EU member state's own version of data protection law and is likely to increase public awareness about the rights ordinary citizens have regarding their own personal data protection. With a wide ranging scope covering many industries, GDPR also has specific coverage for video surveillance data.

GDPR sets out principles for video surveillance data collection, use limitation, security safeguards, individual participation and accountability. Some of the clauses which will apply to video surveillance installations include:

- Public authorities must appoint a data protection officer, an individual who will be responsible for data protection. Private organizations which manage public space video surveillance may also need to appoint a data protection officer.
- Privacy impact assessments (a type of risk assessment) will be required relating to the storing of data from public spaces and some other areas.
- In publically accessible spaces individuals will have the right to request a copy of their data – in the case of video surveillance this means providing a copy of video footage.

For installations in the EU if there are data breaches, the systems manager is legally obliged to notify the authorities within 72 hours of discovery. Failure to do this can result in sizeable fines (up to €20m or 4% of turnover). It may be deemed there has been a high risk of impact on the rights and freedoms of individuals whose data is contained in a breach. If there were not sufficient precautions to protect the data (for example in video footage – encryption or anonymization of individuals) individuals may have case for civil damages. Although without test cases post-GDPR it is difficult to predict the outcome of these cases. Concerned parties should watch this space with interest.

What can be said with certainty is that if unprepared, the requirement in GDPR for organizations to respond to requests for copies of video surveillance data featuring them could overwhelm those organizations. If an organization's surveillance system covers publically accessible areas they may be required to provide a copy of any video footage featuring an individual to them on request. If their system is not optimized for this, this is likely to pose a high administrative workload in validating and processing these requests. Video footage featuring multiple individuals would need to be redacted to protect the anonymity of other individuals. At present many US police forces are engaged in a large number freedom of information requests from the public for body worn camera footage. Image redaction is consuming large amounts resource and budget. For some organizations GDPR could have a similar affect. Technology to automate and assist with the redaction workload such as automatic identity masking video analytics are available. Going forward solutions like this are expected to be utilized by organizations which may be prone to high numbers of GDPR data requests.

Perhaps most interestingly in GDPR is the discussion surrounding data breaches. Video surveillance has already had numerous high profile examples of hacking due to vulnerabilities exploited in several products. GDPR outlines real potential consequences for future data breaches. Risk assessments may lead organizations to place a higher value on the features of surveillance systems which allow for mitigating data breaches such as tools for detection/reporting and additional steps to protect data in case of its unlawful extraction (e.g. encryption). For smaller organizations, if there is going to be additional compliance work for GDPR, it may spur them to use a security as a service provider (not

necessarily cloud based VSaaS) which they pay to manage their system and all corresponding data compliance.

For the surveillance industry the timing of GDPR is particularly interesting. It comes at a time when several EU country markets (in the light of increased terrorism threats) have expanded their video surveillance coverage in public spaces and even increased the use of police body worn cameras. GDPR is seen by many as long overdue legislation from the EU to protect citizen's privacy in the light of all the technological advances of the past 20 years. In many European countries (Germany being a regularly cited example) citizens have long been cautious of greater collection of their personal data. GDPR provides citizens with clearly defined rights to keep organizations from open ended data collection with the minimal consideration of privacy. If unprepared, organizations found to be in breach of GDPR may find themselves subject to large fines from the authorities or perhaps more damaging, potential wide scale legal action from affected citizens.

Big differences between the Chinese market and the rest of the world

By Jon Cropley

China is forecast to account for over 46% of global professional video surveillance equipment revenues in 2018. Despite this, the Chinese market has some unique characteristics that make it very different to other regional markets. This has led to the suggestion there are two markets for video surveillance equipment: the Chinese market and the world market excluding China. Below are 5 ways in which the Chinese market differs from the rest of the world.

1. Supply of equipment is more concentrated in China.

The two largest vendors of branded video surveillance equipment accounted for over 50% of the Chinese market in 2016. This compares to the world excluding China where the two largest vendors accounted for less than 20% of the market.

2. Shipments of deep learning-enabled equipment are much higher in China.

It is forecast that three quarters of all deep learning-enabled servers for video surveillance shipped worldwide in 2018 will be shipped in China.

3. Domestic vendors dominate supply of equipment in China.

Chinese vendors account for more than 80% of Chinese market revenues. There are other countries where domestic brands dominate supply (Germany, Japan and South Korea are all examples). However, in most other country markets, foreign vendors account for a much higher proportion of revenues.

4. Shipments of HD CCTV are proportionally lower in China.

It is forecast that HD CCTV cameras will account for only around 10% of all cameras shipped in China in 2018. It is forecast they will account for over half of all camera shipments in the world excluding China.

5. The market has been growing faster.

The Chinese market has grown at an average annual rate of 13.3% between 2012 and 2017. In comparison, the World market excluding China has grown at an average annual rate of 2.6% over this time.

Despite all of this, growth in camera shipments has been slowing in China as the market becomes increasingly saturated. Continued high market growth will increasingly depend on shipments of higher-priced next generation deep learning-enabled equipment.

Drone detection technologies

By Oliver Philippou

In last year's "Video Surveillance Trends for 2017" white paper, IHS Markit identified the use of drones and robots as a growing technology for security applications. In reality the use of drones (unmanned aerial vehicles) for this purpose has not really taken off because of three main issues; legislation, battery life, and cost.

However, the use of drones has emerged as a very real problem for perimeter security. For would-be intruders or unwanted observers using drones, the issues suffered by the commercial market do not apply. Consumer drones are readily available for just a couple of hundred dollars and flown by anyone with no prior training and without a license. Thus the problem of drones in restricted airspace, such as near airports, critical infrastructure facilities, or above sports stadiums full of spectators, has become an increasing concern.

Given the large physical area that these restricted airspaces cover, simply being able to identify that a drone is nearby has proven challenging. However, IHS Markit expects that recent developments in drone detection technology mean that in 2018 anyone wanting to secure a perimeter will have to take into account the threat from above.

There are currently two main drone detection technologies:

Radio Frequency (RF) detection aerials: These products are used to detect, analyze, and locate the RF used by the drone base station to communicate with the drone. The benefits of RF detection aerials are that they can detect and locate both the drone in the air and the person controlling the drone, in some instances even before the drone takes off. RF aerials are also able to detect over a much greater range than radar or video surveillance cameras. Additionally, RF aerials can potentially even interfere with the communication between the drone and the controller. However, doing this can have unknown effects, such as the drone dropping out of the sky. The problem with RF aerials is that they are not particularly accurate at providing a specific location, nor are they able to provide video verification of a drone.

Radar: Ground surveillance radars are used for low-level aerial surveillance to detect and track small drones. They use a similar technology to air traffic control radar, but on a smaller scale, providing a shorter operating range than RF aerials. However, radar is significantly more accurate than an RF aerial, and therefore is well-suited to be paired with video surveillance cameras including PTZ cameras automatically to zoom in and follow targets. The downside of radar is that performance can be impacted by adverse weather (for example rain, snow, sand or dust). Radar-based drone detection systems tend to be more expensive than RF aerial systems.

Video surveillance alone is not considered an adequate detection technology. Object detection analytics can be used on a video surveillance camera for video verification and capturing a visual image of the potential threat. However, both RF aerials and radar can detect beyond the line of sight, and have nearly a 360-degree field of detection. Therefore many vendors are finding that combining all three technologies together offers the best chance of drone detection. The use of video has an important role to play in this emerging field of perimeter security.

Video surveillance fault tolerance

By Josh Woodhouse

The ability of a video surveillance system to tolerate faults while maintaining operation with minimal disruption is seldom discussed. No one likes to plan for the worst, yet even though the video surveillance industry is increasingly utilizing enterprise grade IT technology, many video surveillance systems still have fairly limited fault tolerance and failover capability. When compared with what is common in the IT industry, the video surveillance industry is often thought of as having a relaxed approach to many aspects of failover and redundancy. However, as the multiple uses and perceived value of video surveillance data is increasing we may see increased demands for greater failover, redundancy and backups from end-users.

Surveillance systems which do have a high level of fault tolerance tend to focus on mitigating failure after video is captured by a surveillance camera. This is due to a higher impact of failure from the "back-end" rather than at an individual camera. For example, if an individual camera fails, the impact is smaller than if the recording server or storage system fails which may cause the loss of all past and future video recordings.

As video surveillance is being leveraged for multiple uses beyond just security the perceived value of video surveillance data is increasing. This value can sometimes be measured with incurred costs if data becomes unavailable. This may be a direct cost (e.g. a fine from an authority) or an indirect cost (e.g. lack of data for business operations, hampering productivity). Cost analysis can form the basis for evaluating potential investment into additional levels of failover, redundancy and backups for video surveillance systems such as:

- Additional hardware costs (e.g. redundant servers / storage).
- Additional software costs (e.g. virtualization or mirroring software licenses).

An interesting example of where we've observed increased levels of failover and redundancy is in legalized marijuana supply in the USA. Here, facility owners are investing more in higher levels of failover in their surveillance systems to ensure they do not fall foul of stringent legislation in some states. This legislation focuses on the ability to retain and produce past video recordings when demanded by authorities. Failure to comply can have dire consequences including loss of business licenses. In other industries, for example manufacturing, as video becomes more ingrained in business operations we are likely to see similar patterns of investment for greater failover in video surveillance systems.

Forensic video analytics as a service

By Josh Woodhouse

When reviewing video for investigations one of the biggest challenges is the sheer volume of video footage which may need to be examined. It's said that typically it may take a trained officer or analyst using traditional methods (a notepad and the pause/rewind buttons) 1.5 - 2 hours to review just an hour of raw video footage. This can be a huge consumer of resource. The problem is particularly prominent in police forces where the issue is amplified by a combination of budgetary constraints and a spike in the amount of video inputs (increased use of body worn cameras and more publically submitted videos). There have long been grounds to find a more efficient solution.

Several video surveillance analytic solutions for forensic video analysis have been available for some time, yet, the improvement in accuracy in the last 18-24 months using deep learning technology has been critical. This advancement has pushed accuracy to a level of competency that can be reliable enough to assist human analysts. However, deploying this technology can prove expensive for police departments. At present there is a significant hardware cost required to run this type of video analytic. And many of the potential clients are not managing live cameras but instead looking for a tool to search through the repository of potential evidence they have collected from multiple sources in many formats.

Some providers have offered use of their analytics and software packages in a "as a service model" where police forces or agencies can utilize the vendor's onsite infrastructure and internal analysts to outsource their forensic video analysis. Moving this model to a cloud platform is an obvious evolution where by following some training clients can use on-demand forensic video analytics for particular cases remotely with their own analysts without large hardware investment.

This is an exciting prospect for some smaller forces, which may not have the available capital for their own infrastructure or a large enough case load to justify a large capital expenditure.

For large agencies and police departments with either highly sensitive data and/or large caseloads their own onsite infrastructure will most likely be the most cost effective solution.

IHS Markit expects that forensic video analytics will be integrated into existing cloud services. For example in the body-worn camera market many police forces already utilize the cloud to store and review body-worn video, yet, in these repositories we still see a degree of separation from other video sources, for example from fixed (public or private) video surveillance. In 2018 IHS Markit expects to see increased convergence in post recording video repositories where, even if only on case by case basis, multiple sources of video will be brought together to be investigated using deep learning video analytics for which cloud may be an important enabler for on demand requirements.

The Xue Liang program, a boost to the Chinese market

By Jackie Zhang

Thanks to the increasing investment in safe cities by the Chinese government, city surveillance is the largest end-user industry in terms of revenue in the Chinese video surveillance market. It is also forecast to exhibit double digit growth through to 2021.

According to the United Nations statistics, of the world's 31 megacities (cities with 10 million or more inhabitants) in 2016, six were located in China. They are Shanghai, Beijing, Chongqing, Guangzhou, Tianjin and Shenzhen. By 2030, Chengdu will have grown to become China's seventh megacity. In the past decade, the Chinese government has invested greatly in public safety through a series of programs to deliver safer cities. The "Xue Liang" program, initiated by the China Central Social Security Administration Committee, is the latest and is expected to be a major driver of the Chinese city surveillance market growth in 2018.

Government policy driving city surveillance growth

The Chinese city surveillance market is mainly driven by the government's guidance and policies. Previous key initiatives include:

- The Skynet Program. Launched in 2005, Skynet was initiated by China Politics and Law Committee with objectives of strengthening public security management by installing surveillance cameras in key public areas such as crowded public areas and the main traffic arteries.
- In 2015, nine ministries including the Chinese Development and Reform Commission issued "the Guideline for Improving the Full Connection of Video Surveillance in Public Area". These guidelines set a series of goals to be achieved by 2020 including:
- Completing the installation of network cameras in all key public areas, key industries and campuses.
    - On-going upgrades of existing cameras to HD resolution in the above mentioned areas.
    - Ensuring all video footage from such areas is accessible to the authorities.

Xue Liang Program to drive ICT equipment deployment in safe cities in 2018

The Xue Liang program was launched in 2016 and is complimentary to the previous 2015 guidelines and is included in the government's 13th Five-year economic plan. Xue Liang, roughly translated to English as "brightness", derives from a Chinese phrase that the "civilians' eyes are bright". The program's name expresses the idea that China's public security can be improved by leveraging civilians' engagement in its management.

The main objective of the Xue Liang program is to connect all the video surveillance cameras which are installed in districts, towns and villages to a central surveillance platform from county level to national level, and build a comprehensive mechanism for video data sharing across law enforcement of both local and central level, emergency services and other government agencies. This will also see the extension of some city surveillance systems into surrounding rural areas.

The biggest challenge of the Xue Liang program is to build an ICT architecture to enable the connection of a large number of surveillance cameras from public and commercial areas, as well as the analytics allowing users such as police departments to interpret the "big data" generated by such a large system.

Cloud storage and computing are essential in achieving the goals of the Xue Liang program. With large datacenter scale compute / storage facilities being required to manage the huge amounts of video data and video analytics as a tool to interpret it. Therefore, in 2018, it is expected that more traditional video surveillance vendors will be extending their portfolios with datacenter ready hardware and cloud-enabled offerings to meet the technology requirements of the Xue Liang program.