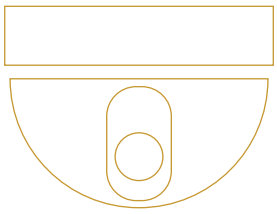
IHS Markit

Top Video Surveillance Trends for 2017

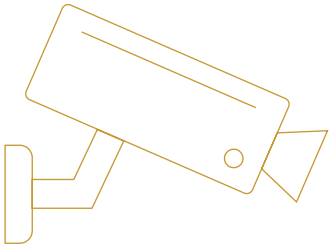
By the IHS Markit video surveillance group

In 2017



98 million

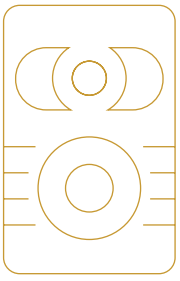
network surveillance cameras will be shipped globally through professional sales channels



Almost

29 million

HD CCTV surveillance cameras will be shipped globally through professional sales channels



400,000

body worn cameras will be shipped to law enforcement agencies globally

Demand for video surveillance equipment is likely to continue growing rapidly in 2017. However, price competition will remain intense. As a result, IHS Markit is forecasting that the world market will grow at an annual rate of less than 7%.

Competition will not make it easy for vendors to grow revenues and margins. Some will fail in this regard and further consolidation of the supply base is inevitable. However, there will be opportunities for well-placed vendors. For example, demand for some camera types will grow particularly quickly (180/360 degree cameras, thermal cameras, and stereoscopic cameras are all examples). Some end-user sectors will also grow quickly. For example, there is likely to be increased investment in border protection and investment in city surveillance spending will continue to be fueled by counter-terrorism initiatives. In terms of geographic regions, the Middle Eastern and Latin American markets are both forecast to grow at higher than average rates.

So, what will be the big stories in 2017? Cybersecurity, deep learning analytics, security drones, and the diversification of Chinese video surveillance equipment manufacturers are just some of the trends discussed in our seventh annual white paper on trends for the year ahead. The predictions on the following are to provide some guidance on opportunities in the video surveillance industry. We hope you find them useful in planning for 2017:

- Video Surveillance Cybersecurity: The industry getting to grips with scale of the threat
- Deep learning revolution
- Chinese vendors continue to diversify
- Body worn cameras: Shift to live streaming
- Droning On! Security drones set to take-off
- HD CCTV demand: High in some countries but not in China
- Safe Cities: The building block of smarter cities
- The evolution of VMS user interfaces

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 / 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
jon.cropley@ihsmarkit.com

Video Surveillance Cybersecurity: The industry getting to grips with the scale of the threat – by Josh Woodhouse

The cybersecurity vulnerability of IoT devices has been a hot topic in 2016 and focus on this subject will not relent in 2017. The threat of a cyberattack was brought to wider public attention in October 2016 when large numbers of infected devices including video surveillance equipment were leveraged in a Mirai botnet DDoS attack. This disrupted service at several internet giants including Netflix, Twitter, Spotify and some large US internet service providers. It also led to fears in the media of similar attacks causing disruption during the November 8th US presidential election.

Cybersecurity is a critical concern for vendors of video surveillance equipment. With the introduction of internet-connected DVRs and then true network video surveillance devices closed-circuit-television lost its "closed" nature. Networking video surveillance systems enabled them to become smarter, have richer feature sets, make footage more accessible and make systems more scalable. Yet some of today's cybersecurity concerns stem from lack of education in an industry sometimes slow to adopt all networking best practices and an ICT mindset.

Some of the vulnerabilities that have already been exploited simply stem from default passwords not being reset or products not being updated with security patches. Realistically, many installers have not changed default passwords to enable simple future access for themselves or their users. Security patch updates for video surveillance devices have often proved labor intensive to implement in an industry where a large part of the installed base, particularly the smaller installations, are still somewhat resistant to ICT style service agreements.

Cybersecurity protection for security equipment is high on the agenda at many industry events. There is a concerted industry effort to educate customers and instill best practices for secure networking of video surveillance equipment. However, changing behavior is often not a fast process. High-profile attacks such as those in October 2016 do at least increase public awareness of the problem.

Highlighting cybersecurity as a product feature or monetizing a secure service can be problematic for vendors of video surveillance equipment. New cybersecurity enhancements can lead users to question the cybersecurity of equipment that has already been installed. Furthermore, it is feared that a company advertising cybersecurity of its equipment will provide hackers with an incentive to target that equipment.

Dedicated cybersecurity products for networking video surveillance equipment are currently rare. There have been a few examples, such as an integrated video surveillance network switch with built-in network security and activity monitoring. Yet, much depends on an installation's set-up and management and the level of involvement from ICT professionals. ICT departments more involved in the installation may be able to leverage existing protection and ICT products they are using elsewhere on their networks.

Like in the ICT industry, value-added partnerships, testing and validation will be critical to the future success of video surveillance cybersecurity. Practical examples include:

- Partnerships with cybersecurity companies – leveraging existing ICT solutions and embedding them in video surveillance firmware and software.
- Utilizing in-house and third-party testing to provide notifications and responses of emerging vulnerabilities.
- Aligning to ISO (and other) standards compliance, certification and best practices.
- ICT security consulting services for integrators and installers.

In 2017, IHS Markit expects to see an increase of value-added propositions from video surveillance vendors specifically targeting cyber security. There is greater awareness of cybersecurity issues than 12 months ago. This will lead to further certification of solutions and partnerships in 2017 focused on a more proactive rather than reactive approach to cyber threats.

Deep learning revolution – by Monica Wang

Applications of video content analysis (VCA) are not new to the video surveillance industry. For some time, VCA technology suffered from over-selling by ambitious vendors who exaggerated the technology's benefits. Early adopters often found the accuracy of the VCA's output was far below promised results meaning low market confidence, especially in signature applications such as face recognition. 2017 will be a step up. Market confidence will be rebuilt by the next generation of VCA – powered by deep learning, high performance computing and big data analysis.

What is deep learning?
Deep learning is the fastest-growing field in artificial intelligence; it can enable computers to interpret large amounts of data in the form of images, sound, and text. Using multiple layers of nonlinear processing units, machines have the capability to learn the feature representations of data unsupervised or semi-supervised. This learning process is also called "training process". With constant training fed by massive amounts of data, machines could improve the accuracy of pattern analysis or classification automatically over time.

What is the implication of deep learning for the video surveillance industry?
Both the deep learning infrastructure and the deep learning algorithms for pattern analysis are becoming available to the video surveillance industry. The latest iterations of Graphics Processing Units (GPUs) provided by vendors such as Nvidia and Movidius (an Intel company) provide the deep learning infrastructure to cameras and recorders. Deep learning algorithm developers create video surveillance dedicated training models to have the machines trained unsupervised or semi-supervised for face recognition, vehicle recognition or other video analysis based on deep learning infrastructure. These technologies increase the efficiency of the VCA software development and raise accuracy through access to faster processing and the ability to learn automatically within video surveillance footage. The ability of deep learning technology to enable adaptive analysis of video and require less calibration of algorithms will drive a big leap in the future use, accuracy and range of applications for VCA technology from 2017 onwards.

However, the road to mass adoptions of VCA, based on deep learning, is not easy. The biggest challenge facing both video surveillance vendors and software developers remains unchanged - each surveillance scenario is different. Even with adaptive and learning algorithms the range of application scenarios is challenging. However, thanks to deep learning, the futuristic type results popularized in films and TV which influences end users' expectations for VCA is significantly closer than ever before.

Chinese vendors – are important to the development of deep learning in video surveillance.
China is the largest video surveillance market in the world. With the numerous large installations of surveillance cameras and massive amounts of video data, the end users in China are eagerly seeking ways to interpret the large amounts of data they collect with VCA, notable examples are the police and traffic departments. As a possible differentiator leading to potential market share gains, the deep learning technologies developed by Chinese video surveillance vendors is evolving towards the development of a full value chain ecosystem including collaboration from GPU providers, software developers, vendors and system integrators.

2016 was the first year to see video surveillance equipment based on deep learning installed for video analysis. Chinese vendors have already installed such products for city surveillance application. 2017 is set to continue the trend with increased sales from this technology in the Chinese market. But how soon to see the massive adoption of the VCA based on deep learning in the next few years will largely depend on the return of investment on this technology perceived by the end users.

Meanwhile, the competitive environment could also be changed by the differentiated VCA product strategies. Unlike video surveillance equipment which has increasingly become commoditized, VCA products can be unique for each scenario. With differentiated VCA products, vendors will have better opportunities to grow in well-targeted verticals aligned with their own core competences.

Chinese vendors continue to diversify – by Monica Wang

The combined market share from the 3 largest Chinese video surveillance brands Hikvision, Dahua, Uniview accounted for an estimated 28.8% of the global video surveillance revenues in 2015, up 5 percentage points compared to estimates for 2014. Preliminary data for the 2016 calendar year suggests their combined market share will exceed 30% for the first time. However, in the face of slowing long-term growth in the video surveillance equipment market, vendors are seeking for new drivers of growth. The following are some examples of the largest Chinese brands strategies to attempt to sustain growth.

Geographic expansion

Hikvision established 4 new subsidiaries in Kazakhstan, Colombia, Turkey and Dubai in 2016, increasing the number of oversea entities to 25. Following 10 new subsidiaries established in 2015, Dahua also added 4 oversea subsidiaries in Canada, Panama, Poland and Hungary within the first half year of 2016, to its 22 existing oversea entities. Total revenues from overseas market for both Hikvision and Dahua during the 1st half year of 2016 grew over 35% compared with the same period in 2015. Following in the footsteps of Hikvision and Dahua vendors like Uniview and Kedacom are also busy with extending their oversea network outside China.

The initiatives of One Belt One Road (OBOR) and Asia Infrastructure Investment Bank (AIIB) also benefits Chinese vendors' development outside China. Proposed by Chinese President Xi Jinping, OBOR with $40 billion Silk Road Fund (SRF) and AIIB are dedicated to supporting infrastructure, resources & energy and industrial capacity development in Asia, Middle East, East Africa and Europe. Partnering with China Engineering, Procurement, Construction (EPC) Firms who contract the projects invested by SRF or loaned by AIIB mean Chinese video surveillance vendors have more chances to sell in their into these projects.

Preferable price is one of the most important factors that drive the Chinese vendors' growth, but price differentiation alone isn't sustainable. To gain more share, the largest Chinese vendors are investing locally and leveraging their large research and development resources to propel rapid rates of innovation, such as embracing deep learning technologies for use in for use in VCA applications.

Product diversification

Chinese vendors are diversifying product beyond traditional video surveillance equipment. Both Hikvision and Dahua have expanded their security drone product lines to include multiple iterations and even anti-drone equipment. The acquisition of UK-based intrusion detection manufacturer Pyronix by Hikvision in May 2016 demonstrates Hikvision's ambition to diversify its offerings in other areas of security and enlarge its presence in Europe.

Chinese vendors are also diversifying beyond security. Hikvision entered the industrial automation segment in 2016 by introducing its industrial logistics robot leveraging Hikvision's own industrial vision technology. Hikvision and Dahua have both expanded their consumer brands – Hikvision's EZviz and Dahua's LeChange offer a range of smart home products. LeChange even launched a miniature humanoid robotic baby monitor. The large Chinese vendors are rapidly exploring the potential in the new segments and are well positioned to benefit from the white-space growth in security and aligned industries.

Body-Worn Cameras: Shift to live streaming – by Dominic Williams

Body-worn cameras appear to have cemented their place as indispensable pieces of equipment among law enforcement agencies around the world. Indeed, the question of whether body worn cameras will see widespread adoption globally has become not one of "if" but rather "when."

Body-worn cameras have the power to modify behavior, reduce liability and speed up prosecution within law enforcement applications. A recent study conducted by the University of Cambridge's Institute of Criminology showed that the introduction of wearable cameras led to a 93% drop in complaints made against police officers by members of the public. As a result this apparent success, several other markets for the technology are now emerging. Corrections officers, paramedics, traffic wardens, ticket collectors, and several other types of end-user which have frequent interactions with the public are now trialing body cameras.

As body-worn camera technology has proliferated, interest in how the technology can be used more proactively has increased. Closer collaboration between

police forces and technology providers has led to greater understanding of the operational requirements. One of the functions that law enforcement agencies want added to their body-worn cameras is live-streaming. Live-streaming of video footage to command centers has the power to transform the body-worn camera from a passive "black box," useful only for the forensic after the fact scrutiny of evidence, to a proactive tool that improves operational awareness. It is easy to imagine the potential benefits for law enforcement officers and commanders in times of crises, such as armed hostage situations or acts of terrorism.

The attractiveness of this functionality may not be limited in its utility to law enforcement, and could serve to make the technology even more attractive in other use cases. Correctional institutions for example, often have to deal with inmate confrontation as well as incomplete coverage of fixed surveillance cameras. In this context, the improved operational awareness offered by live streaming of body-worn cameras could improve the effectiveness of the response to an incident of inmate violence, as well as the day-to-day safety of officers. Live-streaming also has the potential to open up new markets for body worn solutions that may not have been interested in a solution that only offers after the fact review of footage that most body-worn solutions are currently limited to. Activities that would normal require two people to be present in order to guarantee safety or standards (manned rail line inspection for example) could potentially be completed by one person with a body-worn camera thus freeing up human resources and reducing costs.

The viability of live streaming of body-worn camera footage has, up until recently, been frustrated by two factors, both of which are linked to the dependence on cellular networks for the transmission of the video data. First, the amount of data that would be necessary to transmit over these networks would result in prohibitive cost to the end user. Second, cellular networks have traditionally lacked the level of security necessary for the transmission of sensitive information that would be transmitted by law enforcement users. Several companies have now developed the technology required to facilitate the secure transmission of video data at a low enough bandwidth to make live streaming of body-worn camera footage a viable option. Larger body-worn camera manufacturers are following suit and promising to roll out live-streaming within the next year. The ability to live stream footage will become an important feature of any competitive body-worn camera offering, not only increasing the usefulness for existing markets but potentially opening up new ones.

Droning On! Security drones set to take-off – by Oliver Philippou

During 2016 IHS Markit has reported on the noticeable increase in the number of unmanned vehicle solutions on show at security trade shows, and developments on both flying drones (A-UAVs) and ground-based robots (A-UGVs). With unmanned vehicles having been used for military purposes for many years, and the now burgeoning consumer UAV market, the prospects for commercial security applications are extremely exciting and well positioned to grow.

Whilst commercial deployments at present are limited to early adopters, IHS Markit expects that they will continually increase in the coming years, particularly in facilities that cover large areas and have extensive perimeter fences, such as in industrial manufacturing; in the power and utility industry, in pharmaceuticals, in data centers, in the oil and gas industry, in airports, and in government sites.

The ideal security solution would be to have total coverage of a facility's grounds. However, it is often not viable for industries to provide this level of security for their critical infrastructure. Whilst unmanned vehicles will not be able to provide 100% coverage, it is the opinion of IHS Markit that drones and robots are able to act as "force multipliers" to assist security teams, with unmanned vehicles performing routine and mundane tasks; and human security guards performing more specific, human interactive tasks.

There are two main functions for drones and robots deployed in commercial security: guard tours and alarm responses.

Both drones and robots will be used for pre-programmable tours of a facility, to provide round-the-clock roaming security. There are pros and cons for each type of unmanned vehicle. Drones are able to fly at height, and thus provide a large-area overview of the facility, whilst a robot on ground level will have only a similar field of vision as a human. However, a drone is limited by its battery life (typically 30 minutes), whilst a robot tends to have much better endurance; Sharp's INTELLOS (A-UGV) for example, that was released at ASIS 2016, has a reported 8-hour run time. The other benefit of robots over drones is their ability to carry multiple sensors and different cameras. Drones are likely to have only a single high-end main camera, and perhaps an additional visible light or un-cooled

thermal camera. A robot, however, could have any number of cameras, providing a 360-degree field of view; and additional sensors, such as RADAR, LIDAR, CBRNE detection sensors, an array of lights, or 2-way audio. In the future, IHS Markit also expects that they will be offered as a modular design to allow end-users to customize robots to meet their specific needs.

The other major use case for drones and, to a lesser extent robots, is alarm response. This is when an alarm is triggered on the perimeter fence. Drones are able to arrive on the scene quickly and provide live video transmission. This will either deter the intruders, or provide an overview of the situation before manned security guards arrive to try to apprehend the intruders. It is unlikely that robots will be used in this situation as current iterations are slow and would take too long to respond.

IHS Markit currently expects that specialized drone and robots companies will manufacture the unmanned vehicles themselves, with enterprising video surveillance equipment vendors choosing to offer their own video surveillance equipment, either through OEM arrangements or through strategic partnerships with these manufacturers. IHS Markit believes that a key area of focus for vendors of video surveillance products and services will be the user-interface of these unmanned vehicles, as well as the integration of the vehicles' video feeds, other sensors, and the status of the vehicle itself, into a holistic video management system.

Although this market for unmanned vehicles is currently only small, IHS Markit believes it has the potential to grow significantly in the coming years. This technology potentially enables end-users to improve their overall security offering, whilst also offering operational efficiencies.

HD CCTV demand: High in some countries but not in China – by Jon Cropley

Demand for HD CCTV cameras and recorders is forecast to continue growing rapidly in 2017. However, demand is forecast to remain relatively low in China. This is despite the largest vendors of HD CCTV equipment being Chinese companies.

IHS Markit forecasts that in the professional market, shipments of HD CCTV cameras will grow to almost 29 million units globally in 2017. This is from fewer than 0.2 million units in 2012. Furthermore, in a number of countries in 2017, HD CCTV cameras are forecast to account for the majority of cameras shipped. India is one example. Elsewhere, HD CCTV cameras are forecast to account for a much lower proportion of cameras shipped. For example, in the Middle East, they will account for less than a quarter of cameras shipped while in China they will account for only around 10% of cameras shipped.

HD CCTV technology allows users to receive HD footage over their existing coaxial cable and many of the initial barriers to its adoption have been resolved or are in the process of being resolved: HD CCTV equipment has a low price; it offers a much greater cable reach than early products; recorders are now available that can record in multiple formats such as analog, IP, and competing HD CCTV formats; higher resolution cameras are being launched including 4K cameras; and power over coax is coming soon.

So, why is adoption of HD CCTV cameras much lower in China than elsewhere? There are three main factors. First, there are many new buildings in China and relatively little existing coaxial cable installed. Second, the average price of network cameras is much lower in China than elsewhere in the world. Third, while HD CCTV can be a good solution for small systems, it is not as scalable as IP and there are many large projects in China. Taken together, these factors mean that IP video surveillance systems are often chosen ahead of HD CCTV systems in China. Elsewhere, these factors play less of a role. As a result, 2017 will be another year of high growth in HD CCTV equipment demand globally but this growth will continue to vary considerably by region.

Safe Cities: The building block of smarter cities – by Thomas Lynch

"There is no smart city without a safe city" – a term delivered by a Kenyan government official at a safe city event held in Nairobi during October 2016. This sentiment implies improved urban safety is a key component for the development of the cities of the future. Smart efficiencies in a city require an environment with the ability to mitigate, monitor and respond to security threats. As urban risk levels have increased through global instabilities the use of technology to secure urban centers has expanded to use of many different sensors connected through the internet of things (IoT).

ICT and security technologies are offering new ways for governments and emergency services to detect threats to citizens, mitigate and provide an emergency response to them. Connecting previously separate technologies into an integrated system though safe city initiatives can offer benefits including: faster response times, multi-agency collaboration, budget and data sharing, improved civilian engagement and the ability to provide real-time intelligence and communications support to front line services.

The key technologies associated with a safe city include CCTV, command & control, private LTE communications, data storage, ANPR, video analytics and supporting ICT equipment. The impact of governments wanting to utilize the latest iterations of these technologies protecting their citizens is so much so that the global market for safe city solutions was estimated to be over $14 billion in 2016. This is projected to be worth more than $20 billion by 2021.

Big data analytics, increased sensor connectivity through IoT, and the ability to pool and share resources and ubiquitous access through the cloud will all emerge as key themes into 2017 with agencies and governments wanting to ensure that they are maximizing the use and business case to continue to ensure the success of their safe city deployment and ultimately the safety of their citizens and emergency service front line personnel.

India, China and North America offer significant opportunities for safe city solutions having strong urbanization, GDP growth and favorable risk scores. IHS Markit expects to see the continuation of safe city deployments into the Middle East & Africa region, other parts of Asia and Latin America. With Europe generally having a greater prevalence of older installed security and ICT equipment; projects in this region tend to focus on maximizing existing technology whilst upgrading where possible and linking existing disparate systems. Projects in North America and Europe often suffer difficulties in public – private partnerships with complex procurement procedures and disagreements between large numbers of stakeholders

The growing number of safe city reference projects will cause other government and city officials to launch their own projects, ensuring their cities are not left behind technologically or with increased safety risk. Safe cities which pull together many aspects of security technology will give rise to true smart cities, with public safety platforms providing the bedrock for the next generation of transportation, public information, energy management and sanitation systems. Leading to improvements to the day-to-day lives for ordinary citizens.

The evolution of VMS user interfaces – by Josh Woodhouse

How easily users can interact with video management software can have a huge bearing on a system's effectiveness. Usability is everything when it comes to day-to-day operations - from the training required for new operators, the costs relating to forensic video analysis, exporting video evidence or even direct emergency responses – ease of use is paramount.

When it comes to the user interfaces of VMS platforms some interesting concepts have been demonstrated at trade shows in recent years such as, users being able to interact through the integration of gesture control and augmented or virtual reality. Yet, we may be on the verge of a greater, more sudden change through the integration of artificially intelligent (AI) bots. AI bots are software which uses artificial intelligence to provide assistance to users by interacting with users like a human would through speech or instant messages. Bots can automate tasks and take on basic workloads meaning sometimes they are referred to as AI assistants.

In the wider software industry the widespread use of AI bots is the next stage of evolution following the great explosion of apps over the past few years. The integration of artificially intelligent bots as a way to

interact with all kinds of software is going to be a huge trend. It will fundamentally change the way we interact with software every day; be it on our phones, in our homes or on our computers.

Speech-based services such as Amazon's Alexa, Google's Assistant or Apple's Siri have started to open up their platforms to developers for the integration into third-party applications. It will not be long before the integration of AI bots make speaking or using instant messages to interact with software more innate than using a touch screen or mouse or keyboard.

At present, AI bot platforms utilize cloud processing to generate responses. This means there may be privacy concerns in the security industry as some speech services require listening which is "always on": listening for a phrase prior to an instruction such as "hey siri" or "okay google" and in order to process a response data will need to be shared between the application and the cloud. Nevertheless, it is expected that these concerns will be overcome.

AI bots and assistants are already being used in consumer smart home technology with basic speech commands able to control heating or alarm systems. In the professional video surveillance industry we've already seen the effects of the app revolution – most vendors now offer some form of mobile app-based client to interact with their system. AI bots are likely to follow suit. At first these existing apps will be able to be controlled by speech and as this type of interaction becomes more common speech control will filter into the desktop versions of video management software.

Imagine a security control room in the not too distant future in which an operator speaks to their monitor "rewind the live feed 30 seconds"; "show me all persons detected walking past camera 12 in the last 20 minutes" or "show me all the red-pickup trucks to enter the parking lot this morning". This human-machine interaction makes for a powerful vision of the security control rooms of the future. It may become reality sooner than many think.

Jon Cropley, Principal Analyst for Video Surveillance at IHS Markit
jon.cropley@ihsmarkit.com

Follow the conversation **IHS4tech**
Join the **IHS Markit - Security Technologies Group**

3587-ML-1216