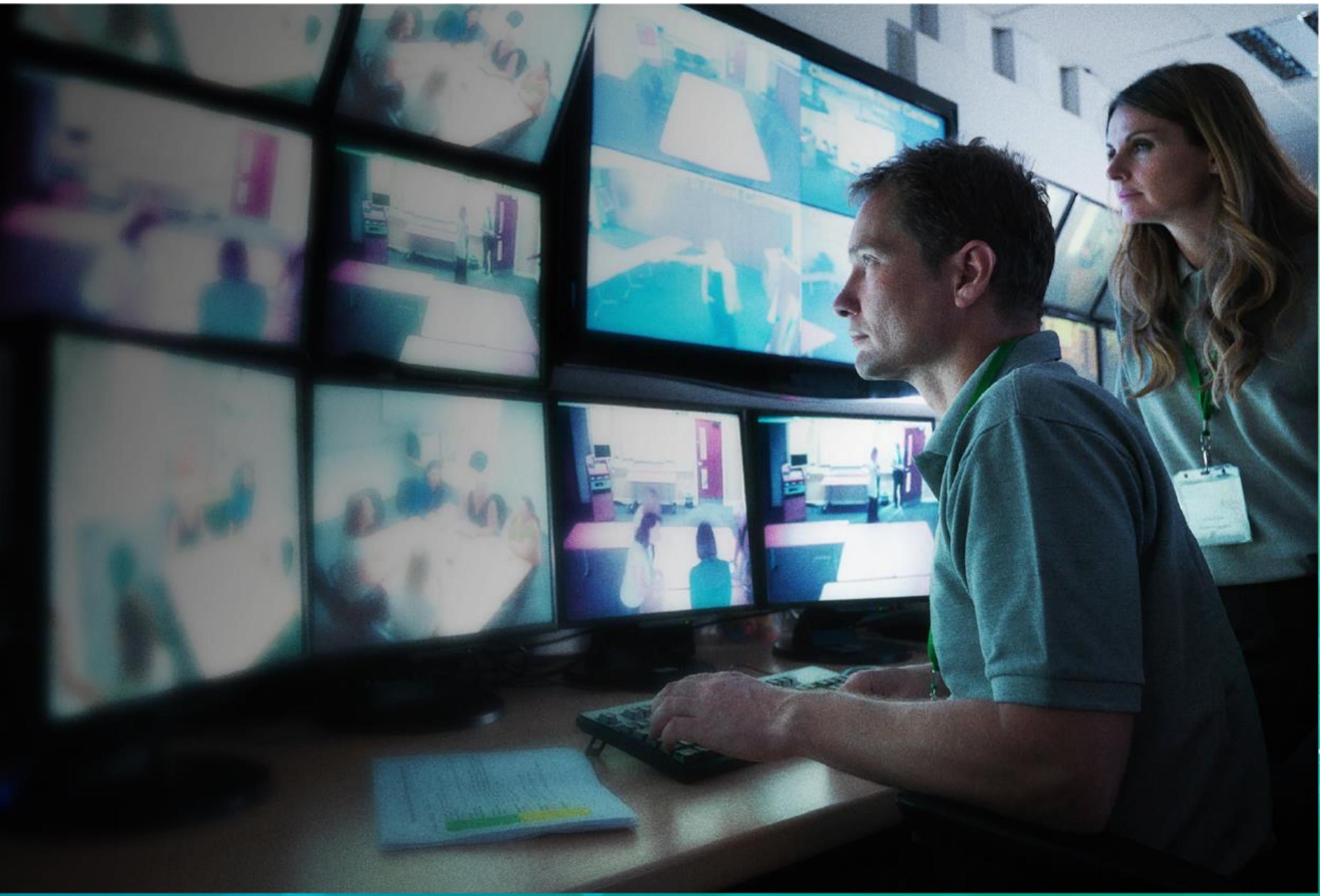
Security Technologies Top Trends For 2019

By the IHS Markit
Security Technologies analyst team



Introduction

For our annual trends whitepaper for 2019 we include trends from analysts covering the video surveillance, access control and critical communications industries.

IHS Markit identified ubiquitous video as one of its top transformative technologies earlier in 2018. In public safety installations, we are observing this concept converge video surveillance and critical communications technologies as personnel embrace the benefits of ubiquitous video. Examples include the latest deep learning video analytics powering insights in safe city installations, a first responder live streaming body worn video to control rooms using the latest mobile broadband networks, or the closer integration and analysis of video data from multiple sources within software applications.

In the wider video surveillance industry demand for professional video surveillance cameras has been growing quickly and is forecast to continue in 2019. 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 180 million will be shipped in 2019. At the same time, the steep erosion in the average price of cameras and other video surveillance equipment is starting to slow. As a result, IHS Markit is forecasting that the world market will grow at an annual rate of over 8% in 2019. Some regional markets, like India and Latin America will grow much faster.

So, what will be the big stories in 2019? Future supply base changes, app stores and use of SaaS in emergency response are just some of the trends discussed in our ninth annual white paper on trends for the year ahead. The predictions on the following are to provide some guidance on opportunities across security technologies. We hope you find them useful in planning for 2019:

- Supply base changes in 2019
- Cybersecurity is more than a political football
- Where are all the GDPR prosecutions?
- Deep Learning analytics at the edge
- App stores for the security industry
- Electronic access control systems: Year-end review and forecast
- SaaS driving next generation emergency response
- Broadband adoption in the critical communications industry
- Licensed mobile radio trends overview

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 service offerings, please contact us.

Jon Cropley

Senior Principal Analyst – Video Surveillance

Thomas Lynch

Research Director – Security Technologies

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

Contact Information:

CustomerCare@ihsmarkit.com

Supply base changes in 2019

By Jon Cropley

Supply to the professional video surveillance market has become more concentrated in recent years. The world's three largest vendors accounted for 17% of market revenues in 2007 and 18% in 2012. In contrast, the top three accounted for 40% in 2017.

Despite this, the supply base for professional video surveillance equipment remains much more fragmented that the supply base for many other markets. There are still hundreds of relatively small video surveillance equipment vendors, many of them with a market share much lower than 1%.

There have been acquisitions in the past decade though. Larger examples include Schneider Electric acquiring Pelco, Hanwha acquiring Samsung Techwin and Canon acquiring Axis Communications. In recent years, many smaller video surveillance software vendors have also been acquired. Examples include Canon acquiring Milestone Systems and Briefcam, OnSSI acquiring SeeTec, Panasonic acquiring Video Insight, and Tyco acquiring Exacq.

Recent years have also seen some acquisitions combining video surveillance vendors and vendors of other security technologies. These have included Hikvision acquiring Pyronix and Avigilon being acquired by Motorola.

There are likely to be further mergers and acquisitions in 2019 as vendors attempt to challenge the three largest vendors of Hikvision, Dahua, and Axis Communications. However, a spree of large scale mergers and acquisitions is not expected.

Furthermore, it is important to remember these three largest vendors have themselves largely grown through organic means. The rate at which they have done this has been impressive. None of these companies were among even the ten largest vendors in 2005 and Hikvision and Dahua didn't yet exist at the turn of the century. This shows just how quickly market shares can change and how quickly new entrants can grow.

There have been several new entrants to the professional video surveillance market in recent years (e.g. Motorola, Eagle Eye Networks, Amazon, Huawei). There will be more new entrants in 2019. Perhaps some of them will be among the market leaders of the future.

Cybersecurity is more than a political football

By Niall Jenkins

Cyber security was one of the buzzwords of 2018. Something of a political football throughout the year, some Western brands looked to cybersecurity to differentiate their offerings from products and solutions supplied by Chinese competitors.

That said, there are real threats that need to be addressed in the cybersecurity market. As devices become increasingly connected and networked, every node on the network has the potential to provide access to a bad actor. Furthermore, the highly resourced and cyber-advanced vendors, such as Microsoft and Adobe, are getting much better at protecting their code from attack. The consequence is that cyber criminals are starting to look at the emerging IoT (Internet of Things) markets, such as smart home and physical security. Combined with the relative inexperience of self-installers as well as security integrators (remember, analog cameras accounted for over 60% of new camera shipments only five years ago), this makes the video surveillance industry a high profile target.

Interestingly, while building technology has been used as a point of entry to steal credit card details, in many cases the cyber-attack is focused on using connected devices to deliver DDoS (Distributed Denial of Service) attacks. These attacks work by spamming chosen websites with requests from thousands, or millions, of connected nodes on the internet, overriding the sites ability to respond and making it crash. These attacks may (but not always) inhibit the ability of the devices to perform their configured function, for example to record video surveillance footage.

In response to all this activity the video surveillance market has started a process of education on cyber security. This has included training sessions and seminars, increased feature sets and best practice guidelines and the deployment of some encryption technologies. However, much like GDPR, there seems to be more talk about cyber security than real action or consequence.

So, what will happen in 2019?

IHS Markit predicts:

- There will be an increasing focus on where components and software is sourced and which OEM partnerships are in place. Software auditing is required by end-users in many critical vertical markets which will make this more transparent.

- In the lower end of the market, ease of use will compete with cyber security. Ultimately, SMB's are not as concerned with cyber threats and will prioritize ease of use and installation over security unless legislated to do something different.

- Which leads to regulations and the lack thereof. The industry will continue to lack real regulation and legislation, instead following the lead of the IT industry and large suppliers such as Microsoft.

- Political interest will continue to impact the cyber market with more broad challenges to Chinese vendors in the telecoms and IT industry spilling over to the video surveillance market.

Where are all the GDPR prosecutions?

By Josh Woodhouse

In last year's "Trends for 2018" whitepaper we discussed the impact GDPR was likely to have on the video surveillance industry. One year on, we assess the situation going into 2019.

Even those reading this from outside the EU will no doubt have seen a flurry of GDPR related emails asking them to update their marketing preferences for various mail lists around May 2018. For many, this will have been the limit of their experience with GDPR. Judging by the large number of emails with tweaked privacy policies, GDPR certainly invoked action from many companies, so with apparent widespread compliance regarding marketing data, what about video surveillance?

Well, for video surveillance systems, the evidence for compliance with GDPR regulations is much less obvious. GDPR replaced the privacy regulations of EU member states, some of which had no specific requirements for video surveillance, some of which did have specific requirements (for example, requiring signing of video surveillance recording and a dedicated contact or data controller). Nevertheless, many of the GDPR requirements applying to video surveillance technology still seem shrouded in ambiguity.

Some video surveillance vendors have marketed features and solutions for "privacy by default" which is a principle of GDPR. These product features include automated image masking video analytics and greater control of user permissions. However, despite some marketing claims to the contrary, there are no official "GDPR compliant" products.

The responsibility to police GDPR principally rests with each EU member states' data protection authority. Over 6 months on from the introduction of GDPR there have still been few test cases which have proceeded to prosecutions or fines. Also, despite some complaints and investigations, to our knowledge there have still been no prosecutions or fines related to video surveillance. An issue faced by the data protection authorities will be the public's increased awareness of privacy regulations and consequently the volume of complaints they now must investigate. This is likely to have put increased pressure on their resources.

Large fines for those found to be in breach of GDPR rightly remain as a deterrent to non-compliance and can promote self-policing of the regulations. However, there remains potential for a class action style compensation campaign against a data breach or deliberate misuse. If this type of action occurs it is most likely to be against a large organization with many affected users such as a social network organization, bank or retailer. If successful, this could lay the foundations for smaller cases such as those likely for video surveillance. Yet, this is still speculative. As we start 2019, the actual impact of GDPR on the video surveillance industry has been small.

The hype surrounding the introduction of GDPR and the growing number of high profile data-breach scandals has put privacy protection at the forefront of many user agendas. Video surveillance vendors which are perceived to be proactively confronting privacy concerns and promoting ethical data use will be well placed to succeed should GDPR regulation have more bite in 2019.

Deep Learning analytics at the edge

By Oliver Philippou

In 2018 deep learning analytics were nearly all processed either on a server or in the cloud, not at the edge. However, 2019 will be the year of the embedded deep learning application specific integrated circuit (ASIC) system on a chip (SOC).

Due to the power requirements of current GPU hardware, deep-learning analytics have typically had to run on servers. However, the transition of deep learning out to the edge has already begun. NVIDIA offers the Jetson embedded computing platform that allows edge-based inferencing. However, the Jetson platform is an all-purpose GPU not specifically designed for video surveillance cameras. Intel's Myriad X VPU is the third generation VPU from Movidius and features the Neural Compute Engine - a dedicated hardware accelerator for deep neural network inferences. Deep-learning analytics are also being deployed exclusively in the cloud using Video Analytics as a Service (VAaaS) solutions with just the simple addition of a gateway edge device.

When deep learning-enabled cameras were first launched in 2016, very few AI chipset options were available. NVIDIA's Jetson and Movidius's Myriad were often used in deep learning-enabled camera product demonstrations. However, high prices and high-power consumption of these chips meant the early specific AI chipsets has limited adoption in cameras. IHS Markit expects that in the next few years, the SOCs designed for network cameras will be capable of performing the basic processing required for deep learning analytics to run on the camera, without the need for additional processing power. The ASIC SOCs will be beneficial for large scale production aimed at the price sensitive mass market. ASIC SOCs with lower power consumption and a more compact design are being developed. Both established semiconductor giants and smaller start-ups are developing ASICs for use in deep learning-enabled cameras increasing competition in this area.

Currently both Ambarella and HiSilicon, a subsidiary of Huawei, are developing ASIC SOCs for network cameras. Ambarella has already released the CV2S SOC, however, this chipset is presently too high priced and overly powerful for mass market video surveillance requirements. It is likely to be used for autonomous vehicles. But, currently in development, and due to be released in early 2019, the CV22s includes CVflow architecture that provides the DNN (Deep Neural Network) processing required for deep learning analytics. Similar to Ambarella, HiSilicon is developing the Hi3559A SOC with a CNN accelerator to allow the processing deep learning analytics; Whilst Qualcomm will soon be releasing the QCS605.

The level of inference is something that can be changed with tradeoffs in features, accuracy, frames rates, and resolution, but IHS Markit expects that ~0.2 Deep Learning Tera-operations per Second (DL TOPS) is enough for a basic classification network with low frame rates. IHS Markit expects that by 2022, 50% of network cameras shipped globally will include a deep learning accelerator that can provide between 0.5 to 2 DL TOPS. This will allow cameras to do basic object detection and classification leading some to describe it as "the motion detection of tomorrow" hinting it will become a standard feature. Additionally, it is not expected that deep learning accelerators will add any significant cost to the price of the SOC's.

It is expected that the development of edge-to-core processing will become significantly more common in the coming years. As such more powerful edge devices will help distribute the required workload. It is not expected that these edge devices will replace the need for central server or cloud processing, but instead will complement each other.

App stores for the security industry

By Josh Woodhouse

An increasing number of vendors are marketing app ecosystems for video surveillance cameras. This is a further manifestation of increased processing power at the edge and a de-centralized architecture. However, apps for video surveillance cameras are not a new concept. The revival of app based ecosystems has synced with the resurgence of interest in video analytics, fueled by deep-learning technological advances. This means many of the new apps available for compatible cameras are based around deep learning video analytics. This was not the case for previous apps.

Notable examples of video surveillance camera app ecosystems announced in 2018 include:

- Huawei's software defined camera.
- The Bosch backed SAST start up and associated Open Security and Safety Alliance.

These are in addition to existing platforms including:

- The Axis Communications camera application platform.
- Cisco IP Camera Apps.

These platforms all offer downloadable software applications onto compatible network cameras through an app store. These all potentially offer the ability to change the capabilities of the camera remotely through downloadable software. Huawei's "software defined camera" name borrows an IT term "software defined" to market this.

Critics of the video surveillance camera app ecosystem concept have raised the following concerns:

- Once system configuration is complete, it is rare that the camera function needs to be changed. For example, the video analytic function or the type of VMS are rarely changed after the camera is installed.
- At present, the majority of surveillance cameras are required for security purposes and need to record their footage for review in case of an incident. It is unlikely these cameras will be suitably positioned for their use to be changed for other applications like business intelligence.

Despite these concerns, having an open standard and operating system specifically for security and IoT devices means different hardware and software vendors can all use the same platform. In theory, this enables easy configuration of best-of-breed components, with more flexibility for changes and tighter cybersecurity controls than just standard interoperability protocols allow. This could also mean system configurations and camera applications are able to change more often due to an easier delivery model provided by the app ecosystem, not constrained by the current more manual and time-consuming processes. With the app store ecosystem allowing for remote direct software sales and even installation, significant investment will be required from each app developer in adequate technical and configuration support. Especially, if they are to build a successful and highly rated app for security and IoT devices.

Regardless of the need for changing software applications on video surveillance cameras, the "app store" model could be a significant disrupter to the video surveillance industry's traditional sales channel and software licensing model. Once different (non-video) IoT devices are also on the same platform and operating system, greater device interconnectivity and convergence is also likely. Despite not being a new concept, app ecosystems could be a disruptive force for not just video surveillance but other security and IoT technologies in 2019 onwards.

Electronic access control systems: Year-end review and forecast

By Bryan Montany

IHS Markit projects that the market for physical electronic access control solutions has grown to over $5.2 billion in 2018. The market has experienced stable and predictable growth rates that have hovered around 6 percent over the past several years. Electronic locks remain both the largest and the fastest growing product type in access control, representing nearly 40% of the global market size for all access control equipment.

While market growth rates have been consistent, technological developments have dramatically impacted the market in 2018. The most prominent trend involves mobile credentials, which are poised to revolutionize the longstanding business model for access control system sales. The mobile credentials market was still in its infancy in 2018, but many end-users are already anticipating a transition to these credentials by installing compatible readers in their systems. By 2020, over 10 percent of all new readers sold in the market will be compatible with mobile credentials.

Other trends to watch in 2019 and beyond include Access Control as a Service (ACaaS), which allow end-users to avoid the need to invest in costly on-site IT infrastructures to support their access control equipment. ACaaS solutions will be particularly popular to support small and mid-sized projects that service less than fifty doors. In addition, Bluetooth Low Energy (BLE) beacons will support geopositioning in an increasing number of the world’s most advanced access control systems. Through geopositioning, the exact location of specific personnel can be identified at any site in real-time.

The top fifteen access control vendors represent more than half of the total size of the global access control market, but there are pockets of opportunity for new vendors, particularly to accommodate small and mid-sized projects. The mobile credential and ACaaS markets will also be highly competitive in 2019 and should attract an influx of new market entrants.

SaaS driving next generation emergency response

By Alex Richardson

The transition toward SaaS, a shift, while very much underway in the consumer and commercial sectors, has been picking up pace significantly over the last year in the public safety sector. Historically, agencies in the United States in this case, had been very hesitant to deploy solutions via anything other than on premises. A confluence of factors is catalyzing this shift, and it was evident at shows such as International Wireless Communications Exhibition (IWCE) and International Association of Chiefs of Police (IACP), that the emergency response software market is heading in a new direction.

The core emergency response technologies, computer-aided dispatch and records management software, are increasingly beginning to be deployed via SaaS. Discussions with these vendors during the IACP conference in Orlando, Florida, United States indicated varying degrees of adoption. Some smaller to mid-sized vendors such as Mark43 and Omnigo had 100% and 90% of new clients deploying SaaS-based CAD and RMS. Larger vendors such as Motorola also noticed an increasing shift as well.

A further trend picking up substantial pace this year was integration capability and analytical functionality. Several vendors including Motorola and Hexagon were offering subscription-based services to products that integrate data from CAD, RMS, surveillance cameras, sensors and other sources onto a common platform. A key goal with these platforms was to leverage and pull together data from all existing infrastructure and systems and bring the data onto one screen. Analytics could then be applied to the data to highlight where crime was a recurring issue, allowing law enforcement to better allocate personnel in the field. Overall, this signals a shift from responsive policing to predictive & preventative policing, and technology is driving that change.

The future for emergency response solutions deployed via SaaS looks bright. Firstly, law enforcement is becoming more open to SaaS due to a better understanding of the functionality, security features and cost & operational benefits of these solutions. Secondly, public safety technology oriented initiatives such as Next generation 911 and FirstNet, are driving a wide-scale revamp to emergency communications both technologically and operationally. With Next Generation 911, proprietary infrastructure is often replaced with hardware and software that has more open architecture. Open systems are more scalable, provide standard interfaces for integration, are less costly to maintain and offer desirable new features. Additionally, they can be shared among multiple agencies when based on Voice over Internet Protocol (VoIP) communication systems.

Solutions deployed via SaaS go hand-in-hand with the aforementioned initiatives, because they promote interoperability and multi-agency collaboration and can address the current gap between capabilities of emergency response technology and what is available in the consumer/commercial sector. There is a huge focus on using business intelligence for public safety to improve operations, resourcing and dispatching efficiency. SaaS is a technology that facilitates the solutions to tackle those challenges, and 2019 will likely be an important year for the continued development of next generation emergency response technology solutions.

Broadband Adoption in the Critical Communications Industry

By Jesus Gonzalez-Medina

With the growing appetite for broadband-enabled data applications, and the increasing possibility of spectrum allocation in many parts of the world, the market for private/hybrid broadband networks for private mobile radio (PMR) users will continue to expand across multiple sectors. As a result, the critical communications industry will move towards a mix of broadband-capable network solutions e.g. private Long Term Evolution (LTE) or the various operating models possible with commercial and private LTE. It is unlikely that users will adopt broadband solutions to the exclusion of existing Licensed Mobile Radio (LMR), but adoption will be along the lines of a complementary service that allows users to communicate across LMR and cellular networks, depending on specific operational requirements.

Indeed, work is progressing on the development of products and services, with an increasing number of manufacturers and commercial mobile operators entering the critical communications market. The second European Telecommunications Standards Institute (ETSI) Mission Critical Push to Talk (MCPTT) Plugtests™ event was held earlier this year, where as well as voice, Mission Critical Data and Mission Critical Video interworking capabilities were tested for the first time. This work is expected to evolve as 3GPP takes more requirements from different sectors of the global critical communications industry on board.

Revenue projections by sector:

- Revenues Utilities **-** From $164m in 2018 to $460m in 2022 – increase of 181 per cent
- Revenues Public Safety - From $2.9bn in 2018 to $6.9bn in 2022 – increase of 140 percent
- Revenues Transport - From $433m in 2018 to $938m in 2022 – increase of 116 per cent
- Revenues Industrial - From $319m in 2018 to $700m in 2022 – increase of 119 per cent

The figures include revenues from Infrastructure, Mobile Services and Applications, LTE Devices, Managed Services and System Integration.

IHS Markit definitions of LTE networks revenue projections:

- **Hybrid:** Revenues attributed to data/PTT over LTE over a combination (hybrid) of private networks based on commercial cellular technology and public commercial cellular networks that have dedicated access enhancements for users.
- **Private:** Data over private networks (100% privately owned infrastructure) based on LTE cellular technology.

Licensed mobile radio trends overview

By Ryan Darrand

Licensed mobile radio (LMR) deployments continue to increase globally, despite the emergence of LTE solutions onto the world stage and 5G on the horizon. Government and commercial sectors increasingly rely on LMR for secure, instant and reliable voice communications, so cost-optimized digital technologies, TETRA, P25, TETRAPOL and other major digital LMR technologies continue to attract investment. The United Kingdom, a pioneer of LTE technology, announced only in 2018 that it would extend its nationwide Airwave TETRA network to at least 2022 to provide mission critical communications to its emergency services despite the establishment of the nationwide UKESN LTE network.

Overall digitization continues in the industry, as the number of digital users exceeded the number of analog users for the first time in 2017. However, there are a significant number of analog users who have not yet converted to digital-radio protocols. The global success of digital technologies has been multifaceted, as multi-tiered options, greater competition and advances in capabilities have provided an increasingly cost-effective migration path from analog to digital communications. Increasing awareness of the benefits of LMR technology for mission-critical and business-critical organizations around the world has facilitated this growth, and users are turning to trunked cost-optimized digital solutions to meet their scalable communications requirements.

The deployment of trunked networks has increased significantly over the last couple of years, as transportation hubs, utilities companies, mines, and public safety and security organizations have adopted the following technologies:

- **TETRA** has proven itself the technology of choice for emergency services, and European public safety and security continues to be the backbone of the TETRA market, although the largest growth will come from the Americas and Asia. As TETRA becomes more popular around the world, it will continue to spread into business-critical sectors, such as transportation, utilities and industrial.

- **Cost-optimized digital technology**, which includes include digital mobile radio (DMR), digital private mobile radio (dPMR), next-generation digital narrowband (NXDN) and police digital trunked (PDT), has also been successful globally. The largest markets in 2017 were North America and Asia, with Asia accounting for half of all deployments. Cost-optimized digital technologies will be more prevalent in commercial sectors in developed economies with nationwide networks, and in public safety and security organizations in developing regions where no nationwide network exists.

- **APCO Project P25 (P25)** will also continue to increase its footprint, with the world's largest single P25 market located in North America, where P25 is the de-facto mission-critical communications standard for public safety and security agencies. Suppliers of P25 continued to enjoy the spoils of continued investment in public safety in North America, with large-scale network upgrades in 2018, like Motorola Solutions contracts to modernize the P25 network in Portsmouth, Virginia, in a multi-million-dollar deal to provide P25 technology to its emergency services and the Harris deal to upgrade the US Customs and Border Protection (CBP) network. North America is forecast to remain the largest global market for P25, holding more than three quarters of the world's P25 users; however, P25 has also permeated elsewhere in the global market.

- **TETRAPOL** continues to attract refreshment cycles, as high-end government agencies rely on the security and resilience that TETRAPOL offers. Examples include the Fort Irwin United States Army training base in California, which opted to upgrade its network with TETRAPOL Internet Protocol (IP) technology in 2018, and a midlife upgrade of the POLYCOM network in Switzerland, which will extend the life of the network to 2030 and beyond.

Competitive LMR landscape

As the digital LMR market continues to grow, the competitive landscape also becomes more intense, as suppliers continue to innovate, invest in research and development, and users are offered more and more viable communications solutions. Over the years, the industry has undergone a process of consolidation and collaboration, with some key acquisitions, including the Hytera acquisition of Sepura in 2017, and a number of Motorola Solutions acquisitions, including Interexport, Kodiak and next-generation 911 software from Airbus DS. JVC Kenwood highlighted its commitment to global LMR markets, acquiring Radio Activity S.R.L. in 2018 and announcing that it plans to buy shares in Tait, a global supplier of P25 and DMR solutions.

Despite market consolidation, the overall landscape has become more competitive. Increased price competition has reduced barriers to entry, and technological innovations have increased the number of choices, either by provider or protocol.

LMR still growing, as LTE gets established

Despite the emergence of LTE technology, LMR adoption will continue to grow, as LTE becomes more established and proves its capability to meet the specific critical voice communications requirements of emergency services. In the short term, LTE will complement critical voice with data, rather than replace LMR altogether, as investment into LTE is required to continue to increase coverage and resilience. Only in the next five to ten years could LTE substitute for TETRA, TETRAPOL or other high-end LMR technologies, as capital investments are considered in nationwide or large-scale deployments.

For more information visit technology.ihs.com

🐦 Follow the conversation @IHS4Tech

Customer care Americas
T +1 800 447 2273
+1 303 858 6187
(Outside US/Canada)

Customer care EMEA
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.