Technology is changing capabilities

SAM DUNCAN

Rapid technological advancements, such as AI, thermal imaging, drones, robots, and facial recognition, are transforming the private security industry. These innovations are not only reshaping security practices and enhancing operational capabilities but highlight the need for improved regulation and better training.

"It's important to understand the history," says Vlado Damjanovski, founder of CCTV consulting firm ViDi Labs.

He says the shift from analogue to digital in the 1990s was a fundamental change, followed by the rapid development of "better resolutions and bigger pictures" – from HD to 4K, and then to 8K resolutions.

The advancements in digital and solid-state imaging devices coupled with the development of sophisticated AI-integrated software in the 2010s gave rise to today's smart systems.

The algorithms behind the AI, called deep neural networks, are inspired by how the human brain works. "Similar is used in modern video content," Damjanovski says. "You teach the camera what a human looks like, what blue looks like, and all these things are condensed into smaller code and loaded in a camera with the capability to do that on the fly in the live video made up of 25 images per second."

In 2015, AI achieved a significant milestone, surpassing human capabilities in detecting objects with speed and accuracy. According to Damjanovski, this breakthrough has greatly enhanced the effectiveness of surveillance technology, enabling it to reliably alert operators to current, unusual events or activities in extensive surveillance networks where monitoring every camera manually is not feasible.

He says it's also highly effective in reactive applications, which involve constant 24/7 recording and where incidents are typically reviewed the following day. While this process was manual in the past, AI now enables rapid identification and tagging of such events.

Beyond surveillance systems, Damjanovski says another significant shift in security technology is the trend towards the integration of various systems, which has implications for installation and usage.

ASIAL has developed guiding principles for the ethical use of automated facial recognition

At the household level, this integration is evident among the technologically curious, who are increasingly incorporating Internet-of-Things (IoT) devices into their homes.

In larger industries, such as defence and rail, the push for integration has led to more sophisticated system interconnectivity, says Damjanovski. The integration of various security components, such as video surveillance systems (VSS), access control, fire protection, and building management systems, is now becoming more standardised.

He says the integration of intelligent technologies is changing the roles of security professionals. Control room operators now oversee a range of parameters, from traditional security surveillance to monitoring utility usage like water and gas, lift management, and even tracking environmental conditions such as server room temperatures to ensure the longevity of equipment.

This expanded scope requires operators to not only stay alert to potential security threats but also to manage and respond to various alarms that are critical to the efficient functioning of the facility they are monitoring.

John Fleming, general manager of the Australian Security Industry Association Ltd (ASIAL), the peak body for security professionals, says the security market continues to change, driven by evolving threats and changes in businesses and the regulatory landscape.

Cyber is one of the biggest new threats, he says. "Regardless of where you are, everyone is vulnerable to cyber-attacks. When a security system is installed to protect people and assets, a key consideration now is the 'cyber hygiene'."

There are also newer technologies that, not too long ago, seemed futuristic but are now available in the market and are changing how the security industry operates.

Fleming says for vital assets requiring surveillance, access control, and security, thermal imaging cameras are emerging as an important capability. These cameras can effectively operate from distances of up to 400m using edge analytics to determine the image and are not affected by the weather.

He says there's also an increasing use of drones and robotics in surveillance, which enable quick coverage of large areas and provide real-time video feeds back to security personnel.

"For sensitive areas like airports, power plants and military installations, rather than patrolling, a drone can be more cost-efficient," he says. "If there's an event at any level, you then still send a physical patrol."

In situations deemed risky, deploying a robot can be a safer alternative. Equipped with various sensors, these robots are capable of patrolling predetermined routes dynamically due to integrated AI.

They are particularly useful in office blocks, says Fleming, where they can be monitored through cameras and even communicate with personnel.

With the ability to operate 24/7, they periodically return to a charging pad, switching with another robot to replenish batteries.

One innovation that can elicit fear is automated facial recognition technology, and the significant implications it raises.

Fleming says it's increasingly being used in entertainment venues, pubs and clubs, and also in airports at border security checkpoints. "When properly implemented, it works well," he says, citing its use in passport verification and in stadiums to identify banned individuals. "A number of retail stores recently got into trouble, as they did not clearly inform customers that their biometric data was captured.

"Transparent processes must be in place related to the collection, sharing, storing or indeed deletion of biometric data," he says.

ASIAL has developed guiding principles for the ethical use of automated facial recognition to address these issues.

These ethical considerations highlight a need for specialised training as new technologies emerge, which both Fleming and Damjanovski say will be critical to ensuring security professionals have the right skills.

Looking to the future, Damjanovski says algorithms and software is where the next quantum leap will be. "Perhaps beyond object detection and classification, and into detecting and warning of unwanted or dangerous activities," he says.

Time for action on national security

BRYAN DE CAIRES

Australia's $11bn private security industry performs a vital and growing role in the safety of our society.

As illustrated by the growth in the number of licensed security personnel mushrooming from 37,372 in 1996 to 155,562 in 2022 – a 316 per cent increase.

Whether installing and maintaining alarms, video surveillance, access control, security systems, and physical security, providing cyber security solutions, protecting critical infrastructure, defence bases, airports, government buildings, shopping centres, hospitals, schools, crowded places and venues, the services provided by the private security industry touch every facet of our day-to-day lives.

In short, a strong and professional security industry is a fundamental part of Australia's national security mix.

Yet despite this and the unequivocal findings of numerous inquiries and research studies over more than two decades, including agreement in 2008 by the Council of Australian Governments to implement nationally consistent security licensing standards, progress in achieving a national approach remains elusive.

With the protective, electronic, physical, and cyber security sectors forecast to experience strong continued growth, reliance on the services provided by the industry will only increase.

Ensuring there is a professional security industry with the capability and capacity to respond to future demand requires a coherent national approach and strong government leadership. The slow progress over more than two decades reflects a lack of government leadership and a lack of understanding of the important role the industry performs.

By any objective measure, the current regulatory status quo is unacceptable with variations between jurisdictions creating inherent vulnerabilities.

It is difficult to accept that governments would tolerate these inconsistencies despite repeated calls from industry through the Australian Security Industry Association Limited (ASIAL) to address them; as the roll-out in 2022 of Automatic Mutual Recognition starkly illustrated.

While several jurisdictions implemented AMR, NSW, Victoria and West Australia obtained five-year exemptions citing concerns over public safety.

As the peak body for security professionals in Australia, ASIAL is committed to raising professional standards across the industry. A nationally consistent approach to security licensing standards provides a logical way forward in advancing professionalism and building security capability. The current patchwork of security regulation imposes unnecessary red tape and significant compliance costs on businesses operating across multiple jurisdictions.

This creates artificial barriers to competition, restricting workforce mobility and limiting the industry's ability to rapidly respond to market demand.

Achieving a more productive economy is the key to improving living standards. Reducing red tape and improving regulation through the introduction of nationally consistent standards is an important step towards achieving this aim.

As a catalyst for change, ASIAL has drafted a "Model" National Private Security Act which seeks to initiate national discourse in advancing implementation of nationally consistent regulatory standards for the security industry.

The "Model" Act seeks to provide a balanced and consistent framework to engage with stakeholders in advancing nationally consistent professional standards, including:

- Advancing professional standards and strengthening industry capability as part of Australia's national security mix (including requiring cyber security technicians to, as a minimum, meet probity requirements);
- Providing consistent expectations, obligations and responsibilities for individuals and organisations operating in the Australian security industry;
- Addressing public safety concerns over issues such as probity, individual and business suitability, fingerprinting, training, the use of criminal intelligence, compliance and access to a national register of security licence holders;
- Reducing red tape and unnecessary administrative costs;
- Providing industry with greater national operational flexibility and resource management;
- Providing security providers and licensed individuals with greater mobility in responding to surge demand;
- Providing clients with greater confidence when engaging a security provider due to the implementation of nationally consistent standards.

The benefits of a nationally consistent approach to security industry regulation include higher professional standards and improved customer outcomes.

In short, Australia's national security capability and capacity would be significantly enhanced through a nationally consistent approach to security licensing, as indeed would public safety.

Strengthening professional standards through nationally consistent regulation is widely acknowledged as an important step towards building private security industry capability and capacity.

In a changing security environment where cybercrime, organised crime, terrorism and geopolitical tensions pose ever evolving threats, strong leadership is required to bring about change.

Doing nothing is not in Australia's national interests.

ASIAL is calling on federal and state governments to work with industry to bring an end to decades of inaction and finally implement nationally professional standards for the security industry.

Bryan de Caires is CEO of the Australian Security Industry Association Limited (ASIAL).

Private security's $11b contribution to economy hinges on diversity and skills

SAM DUNCAN

The private security industry is an essential yet often underappreciated component of national security and the Australian economy.

Amid growing demand and the emergence of new technologies, cultivating a workforce that is sufficiently large and adequately skilled will be vital for the continued safeguarding of public and private interests, according to industry experts.

Reflecting its significant role, the industry currently employs approximately 200,000 people across Australia in 12,500 businesses and contributes $11bn to the economy.

"Our workforce is larger than the ADF and all police combined, which highlights its importance in keeping people safe," says John Gellel, President of the Australian Security Industry Association Ltd (ASIAL), the peak body for security professionals.

Without full and stable employment in the industry, "we would no longer be the safe country that we are", he says.

The primary function of private security is to safeguard personnel and buildings, and it's often perceived by organisations as a more dependable form of protection, says Gellel.

In Australia, almost every government site, except a few such as Parliament House, are managed by private security.

Private security companies also play a key role in keeping cities safe, tasked with monitoring safe city surveillance systems and reporting incidents to police.

"The relationship between police and private security has evolved, and private security is now seen as an extension of the police," Gellel says.

Over the last 25 years there has been consistent growth in the industry, he says.

The current demand surge has been driven by large public events like concerts and the upcoming Brisbane Olympics in 2032, which pose challenges for police forces alone.

Additionally, he says demand for cybersecurity personnel has surged, adding to the diverse workforce needs of the industry.

Jacqui Loustau, founder and executive director of the Australian Women's Security Network (AWSN), says a major obstacle to attracting sufficient individuals to careers in private security is public perception.

"Many don't see it as a viable career option due to a lack of role models and stereotypical imagery," she says.

"If you Google cybersecurity, you get an image of a person in a dark room in a hoodie."

On the topic of diversity, she says that only 17 per cent of cybersecurity professionals are women.

Gellel says in areas like the installation side of electronic security, female representation is less than 10 per cent.

In protective services, the percentage of women is slightly higher, around 15 to 17 per cent, he says.

"This is a huge issue," says Loustau, emphasising the critical importance of diversity in mindsets and opinions within the security sector, especially for emerging technologies and solving business problems.

"Many of the criminals we're trying to protect our country's organisations and people against are diverse, so we need to be thinking in a diverse way," she says.

Making diversity visible is key to addressing this issue, says Loustau, citing the positive impact of the television drama CSI Cyber on the number of women interested in digital forensics, and the influence of the rise of the Matildas on women's interest in soccer as examples.

Gellel says: "If we're not capturing the total market potential in terms of human resources, we'll always lag behind as an industry."

With its diverse specialisations, including protective services, cybersecurity, and electronic security installation, Gellel says people often overlook the exciting aspects.

Attracting adults to a career change is key, says Loustau, for more than just workforce size. For instance, lawyers are methodical and understand risk, nurses excel under pressure and know how to triage, and marketing professionals can effectively communicate security needs to a company's board.

> The relationship between police and private security has evolved
>
> JOHN GELLEL
> PRESIDENT OF THE AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LTD (ASIAL)

To make security trades more visible, particularly to young people, ASIAL has established a careers portal.

It's aimed at attracting new entrants but can also help security professionals bridge the skills gap created by new technology.

"The careers portal provides career pathway information in protective services and electronic security, with informative videos and over 30 fact files," says Gellel.

"Each fact file provides information on the job description, what they can expect in their role, entry qualifications, and expected salary and benefits."

ASIAL has also drafted a National Private Security Act (NPSA), in a push to achieve consistent regulation across jurisdictions, including training and licensing requirements.

Gellel says this act, intended to address the vulnerabilities created by a patchwork of security regulations, would include training on emerging technologies and be overseen by relevant federal or state departments.

Beyond training, the act aims to address how the current jurisdictional inconsistencies restrict workforce mobility and limit the industry's ability to rapidly deploy personnel in response to emergencies and major sporting events.

Despite some of the challenges, Loustau says a career in private security is highly rewarding.

"It's exciting; it is constantly changing, so you're learning new things, and it's something where you can make a difference and do anything anywhere in the world, and you'll never get bored," she says.