AFP
AUSTRALIAN FEDERAL POLICE

POLICING FOR A SAFER AUSTRALIA

STRATEGY FOR FUTURE CAPABILITY

MARCH 2017

CONTENTS

COMMISSIONER'S FOREWORD

I think this work points to one key word, albeit with different connotations, that best encapsulates why the AFP must evolve and what it must be in the future – 'dynamic'.

In the nearly 40 years since the formation of the AFP, it has evolved from a small agency with a defined remit to a $1.4 billion enterprise with a broad range of responsibilities.

Over this time, the AFP has developed a history of success by rising to challenges and quickly responding to new threats to Australia and Australians. It is a strong heritage of which all AFP members and the Australian community should be proud.

Reflecting on the past few years alone, our achievements have included record drug interdictions, disrupting those intent on large-scale harm and destruction; protection of Australia's children from exploitation; rapid expansion of our international operations; large-scale responses to disasters in Australia and around the world; deployments to conflict zones; significant fraud investigations; and the successful response to new roles in aviation and protection.

Throughout this, the AFP has found new ways to deliver new and improved outcomes – from moving beyond interdiction to broader disruption strategies, from identifying criminality to successfully undermining the financial motives and resourcing for such activity, and from reacting to crime offshore to building our partners' capabilities and strengthening their policing regimes.

The AFP has proven itself as a key element of the Australian national security landscape, delivering quantifiable and substantial reductions in both the direct and indirect harms experienced by individual Australians and Australian society. When realised, these harms can have profound effects: they can undermine public confidence and have substantial economic implications, and may influence our social interactions and inclusiveness.

This paper is not an attempt to define the future crime environment but to understand the factors that will influence the AFP as it approaches and moves beyond its 40th year. It is an assessment of what the AFP and its people, processes and technology must reflect if it is to maximise the value it provides to the community and governments in its continued efforts to reduce those harms.

Since the original tenets of modern policing were outlined by Sir Robert Peel almost 200 years ago, it would be fair to say that countless words have been written about the policing environment, what policing should be, how police services should be structured, and when and how they should change.

Notwithstanding previous specific and external reviews of the AFP and its elements, this paper and the *Future Directions Strategic Context Paper* that preceded it are different in that it is the first time the AFP has taken such a comprehensive look at itself, its environment and its future.

I think this work points to one key word, albeit with different connotations, that best encapsulates why the AFP must evolve and what it must be in the future – 'dynamic'. This word describes both the nature of our operating environment and why we must change. It reflects the posture we must take and how, as a critical national security agency, we must act in that environment.

It is fair to say that many of our stakeholders – with whom we engage on specific issues – were surprised by the true breadth and depth of the AFP's operations and responsibilities. These span local, national and international policing, making the AFP unique among Australian law enforcement agencies.

Many of the true drivers of change in the crime environment at all of these levels have not changed since the earliest origins of policing. Criminals of all sorts will always look for ways to extract a reward through interactions between people or entities, willing or otherwise, known or otherwise. This reward can and always will take a multitude of forms – personal, ideological, financial, and so on.

The fundamental difference now is the rapid pace of technological, social, political and demographic change. It creates a truly dynamic operating environment in which the nature of interactions can change quickly and the opportunities for harm can proliferate and easily transfer from one jurisdiction to another. It can redefine the nature of the interaction, the extent of the rewards and the magnitude of the threat.

...the dynamic environment will continue to challenge generalist policing and standards required of police.

The AFP must respond to this environment by building ‘dynamic’ even further into its organisational DNA. This paper is clear that we must embrace technology-driven transformation opportunities and find a way to resource and deliver innovations that can build our capacities and capabilities over time. This will be particularly critical to responding to the increasing opportunities and challenges of the ongoing datafication of our society and the policing environment.

The paper is also clear that the dynamic environment will continue to challenge generalist policing and standards required of police. Policing will always be a core capability for the AFP, and we must provide the systems, technology and capabilities that can drive continuous improvement in uniform and national operations and allow for new and innovative investigative approaches.

However, there will be an increasing need for specialist skills and knowledge and we will need to work to build and maintain these over time, including with industry and our partners. The AFP can be justifiably proud of its technical and scientific capabilities, which will become increasingly important in a world dominated by technology. Conversely, in some cases traditional technical skills, such as surveillance and covert operations, may offer an advantage when technology challenges us. We must recognise that limitations in these specialised and technical capabilities will have implications for how quickly, efficiently and effectively we can deliver operational outcomes.

We must also work to develop a dynamic workforce that reflects the standards and values of the Australians we serve. This will involve an ongoing focus on cultural reform of the AFP, ensuring it is delivered by inclusive, respectful and constructive leadership. This is the cornerstone of the future AFP.

Lastly, it is clear that our role as Australia’s international policing agency will continue to be critical to remaining dynamic in an increasingly globalised environment. While technology will continue to deliver opportunities for closer international engagement, we will need to maintain a keen focus on shaping this capability through a world-class liaison officer network and key offshore deployments. These have and will increasingly deliver outstanding results for us and our stakeholders.

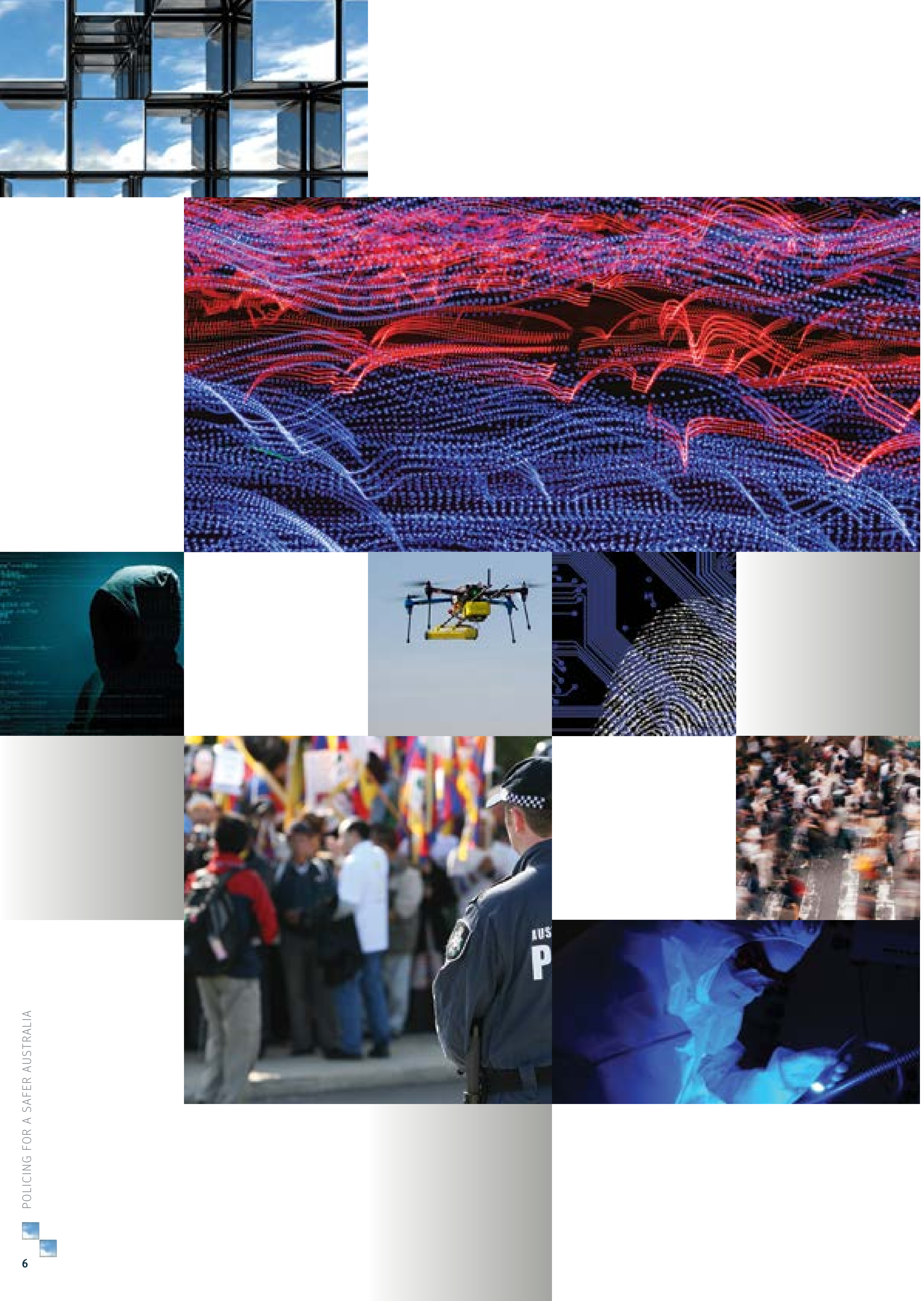
This paper is not intended to provide all the answers to the dynamic AFP we must become. It is another step in a long-term reform journey reflecting my firm view that, while the AFP has proven adaptable and successful, the time has come for a transformation.

This journey commenced with the release of the *Future Directions Strategic Context Paper* and the capability-focused restructure of the AFP in mid-2015. Since then the work surrounding this paper has informed, and been informed by, the underpinning elements of a broader transformation of the AFP.

I have now established an Enterprise Transformation Office to deliver a formalised agenda for this work in consultation with our stakeholders. This will require ongoing discussion with government about the AFP’s role and priorities to ensure that the Australian people continue to get the best return from their investment in their national policing agency.

As a final note, I would like to acknowledge the large number of AFP employees and other stakeholders who have actively contributed to this process. This reflects well on the regard in which the AFP is held and underscores the depth of the commitment to ensuring this agency continues to be the best it can be.

Andrew Colvin APM OAM
AFP Commissioner



EXECUTIVE SUMMARY

A fundamental purpose of policing is the protection of human rights.[1] The AFP's policing and law enforcement responsibilities range from countering international organised crime to community policing, and from deterring and prosecuting terrorists to international peacekeeping.

However, its resources are finite, so it must seek to understand the social, technological and economic environment in which criminals and police will be operating over the next five to 10 years if it is to define its mission properly.

Globalisation characterised by a high degree of interconnectedness involving the easy, rapid movement of people, goods and capital has shaped international society over the past 30 years. In the process, economic activity has moved well beyond single jurisdictions and value has shifted from physical to digital assets.

The technologies that made globalisation possible have allowed non-state actors, from ordinary citizens and small businesses to criminals and terrorists, to operate at a distance and across borders. They have provided criminals with much bigger pools of victims, allowing them to collaborate with anonymity online and to operate from foreign safe havens.

Despite the emerging resistance to globalisation in many parts of the developed and developing world, the technologies that made it possible cannot be uninvented and powerful new ones are appearing.

In Australia's immediate neighbourhood, political and environmental stresses, including signs that some state actors and crime groups are aligning their strategies, will reinforce demands for policing development and humanitarian assistance in the Indo-Pacific region.

All of these developments are shaping the policing environment for the AFP in challenging new ways.

As early adopters of technology operating in an ethically unconstrained environment, criminals (including terrorists) will use new technological capabilities to redesign crime to exploit political, social, economic and legislative vulnerabilities.

Cybercrime is facilitated by encryption, alternative banking platforms and virtual currencies. The vulnerability of newly connected devices in the rapidly expanding 'internet of things' (or IoT) will open up new criminal opportunities, while automated technologies such as robotics will make it possible to conduct personless crime from remote locations.

Other technologies have the potential to undermine the dependability of traditional forensic evidence, such as fingerprints, DNA and signatures. New forms of biological and chemical enhancement will permit the creation of stronger, faster and smarter offenders.

As more and more evidence resides offshore, these developments challenge the traditional single jurisdictional view of law enforcement and global legal frameworks, which are focused primarily on nation-states. In this new environment, the time frames for dealing with crimes will tighten and the complexity of investigations will increase.

The AFP will need more effective strategic planning, resource certainty and the capacity to allocate resources flexibly. It will need to become more technologically capable, drawing on new and more specialised skills and resources. It will be essential for the legislative framework under which the AFP works to keep pace with the rate of change.

Standard AFP investigations will increasingly draw upon multidisciplinary and multi-agency teams, comprising detectives and professional staff. This will require more intense interaction with industry and the research community and will be assisted by investment in technically focused capabilities that can be shared with the AFP's state, territory and Commonwealth partners.

Prosecutorial action will remain a primary deterrent but, with so much criminal activity located offshore, prevention and harm-reduction strategies will become increasingly important. For this reason, new performance indicators that measure success qualitatively as well as quantitatively, based on the effective deterrence and disruption of crime, will be needed.

The AFP's investigative activity will focus on protecting Australians and Australian interests from the impact of transnational serious and organised crime, terrorism and violent extremism.

As the principal international representative for Australian policing and law enforcement, the AFP will increase its effort to lead and coordinate multijurisdictional operational activity through its national and international offices.

It will need to provide deployable international policing capabilities that enable the Australian Government to deliver immediate stability operations, short-term emergency responses and long-term regional policing capacity development when required.

Irrespective of future advancements in technology, policing will continue to be a people-centred profession. The AFP will continue to recruit and develop a flexible and multi-skilled workforce, comprising individuals who are capable of critical thinking, reflection, analysis and independent judgement. In particular, it will need skilled and experienced investigative teams with higher levels of technical expertise, more of whom will be cyber specialists.

It will also need to provide the tools to support its people and a comprehensive skills and qualifications framework to train them. The AFP should assume a greater leadership role in the delivery of national investigative standards and training curricula for its Commonwealth law enforcement partners.

In a competitive employment market, in which new entrants will have different approaches to lifetime work patterns, recruitment will need to be geared towards multiple entries from apprentice to graduate pathways, and more flexible employment models will be required.

The AFP will need to be a valued employer, strongly committed to an ethical, values- driven culture that embraces diversity, inclusion and mutual respect.

LEADING POLICING IN A CHANGING WORLD

A STRATEGY FOR THE AFP'S MISSION AND CAPABILITY

SECTION 1

THE AFP'S ROLE AND FUNCTIONS

The AFP has an extensive and growing range of local, national and international policing responsibilities: from crime reduction in the suburbs of Canberra to disaster relief in the Pacific Islands; from global cyber and terrorist threats to the protection of individual identity.

The AFP's functions include the provision of:

- police services in relation to the laws and property of the Commonwealth (including Commonwealth places) and the safeguarding of Commonwealth interests
- police services in relation to the Australian Capital Territory, the Jervis Bay Territory and Australia's external territories (Christmas Island, Cocos (Keeling) Islands and Norfolk Island)
- protective and custodial functions as directed by the minister
- police services and police support services to assist or cooperate with an Australian or foreign law enforcement agency, intelligence or security agency, or government regulatory agency
- police services and police support services in relation to establishing, developing and monitoring peace, stability and security in foreign countries.[2]

The AFP's current strategic priorities, guided by the relevant minister[3], include leading or contributing to efforts to :

- counter the threat of terrorism and violent extremism
- prevent, deter, disrupt and investigate serious and organised crime activities
- contribute to Australia's border management and security, particularly by protecting Australia from people smuggling
- contribute to Australian international law enforcement interests
- counter the threat of cybercrime
- ensure aviation security
- protect specified individuals, establishments and events at risk of security threats
- disrupt the operation of criminal gangs and the proliferation of child exploitation material
- disrupt the trafficking, distribution and sale of illicit drugs and reduce harm caused by illicit drugs

- protect Commonwealth revenue
- coordinate effectively with the Attorney-General's Department on law and justice aid issues
- prevent Australia from becoming a safe haven for proceeds of crime, corruption and money laundering.[4]

To respond to this broad array of responsibilities, the AFP has developed a professional workforce with an exceptionally diverse set of skills.

Who we are

6,657staff

3,481 police

672 protective security officers

2,504 technical experts, specialist and support staff

74%staff

say they expect to stay with the AFP for the next five years or more. The staff turnover rate is 2.6%.

The average age of AFP staff is

41 years

Diversity

1.6%

of our staff identify as indigenous

35% of our staff are women

22% Sworn

10% Protective Service Officers

60% technical experts, specialist and support

Where we work internationally

57

Australian locations including territories

73

staff work in 28 countries in our international liaison network

190

staff work in eight international missions in the Pacific, Timor-Leste and Cyprus

Source: AFP Annual Report 2015–16.

Purpose and structure of this paper

Policing always reflects, intensely and immediately, the changes and pressures at work in the wider community in which it operates. If the AFP is to understand fully the nature of criminality and the developments that facilitate crime, and to respond effectively, it needs to understand what is driving change in society and how society perceives those changes.

It is never possible to predict the future with certainty, but it is nonetheless dangerous to avoid thinking about it. The purpose of this paper is to examine some of the major global political, social and technological trends that will have an impact on the policing, law enforcement and other responsibilities of the AFP over the next five to 10 years.

Following on from the AFP's 2015 *Future Directions Strategic Context Paper*, this paper addresses the world in which the AFP will have to operate – a world affected by globalisation, changing technologies, population growth, migration, international conflict, failures of governance, violent extremism, climate change and a growing demand for resources.

Section 2 – A more complex operating environment looks at the broad systemic and technological changes in the international environment and Australian society over the next five to 10 years that are likely to affect the AFP and to shape the requirements the government has of it.

Section 3 – Implications for the AFP examines the implications of these developments for the demands likely to be placed on the AFP.

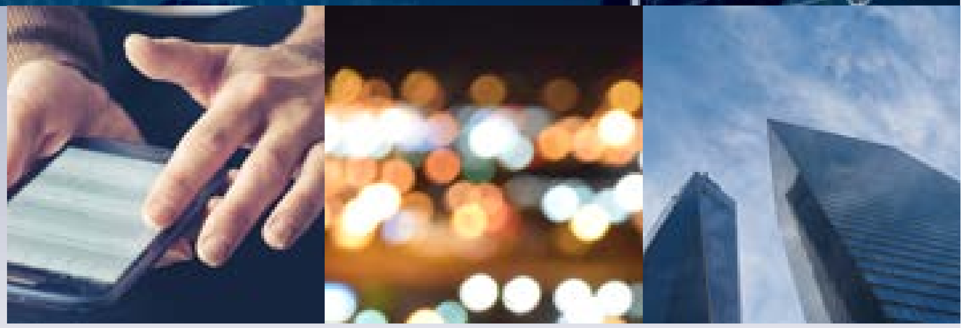
Section 4 – The way forward addresses what they mean for the AFP's mission.

It is never possible to predict the future with certainty but it is nonetheless dangerous to avoid thinking about it.

A MORE COMPLEX OPERATING ENVIRONMENT

SECTION

2



GLOBALISATION

Globalisation has been the defining shaper of international society over the past 30 years, linking people, neighbourhoods, cities, regions and countries more closely than ever before and driving unprecedented new flows of people, information, ideas, and goods and services.

It has been enabled by a revolution in information and communications technologies involving digitisation, mobile telephony, personal computing and social networking.

Globalisation has transformed the international economy by reducing to near zero the cost of transferring information around the world. By freeing the movement of capital and making possible the development of global manufacturing supply chains, it has brought sustained aggregate growth to the developed world, including Australia, and made it possible for large areas of the developing world to participate fully in the global economy. Globalisation has helped reduce the number of people living in poverty around the world by more than 1 billion[5] since 1990. Information and data flows now account for more growth in global GDP than trade in physical goods.[6]

Demographic change and migration

Globalisation has also encouraged and facilitated worldwide urbanisation. For the first time since humanity's shift into cities began some 10,000 years ago[7], more than half the world's population now live in cities. The proportion is expected to rise to 66 per cent by 2050[8] and cities themselves will grow in size as more megacities, develop.

Currently, more than 80 per cent of Australia's population live in its 20 biggest cities, and the majority of our future population growth is expected in and around the capital cities.[9]

Globalisation has also assisted and driven an unprecedented movement of people. In 2014 more than 230 million people lived outside their country of origin.[10] The number of international migrants has grown rapidly over the past 15 years[11], propelled by both economic drivers and conflict.[12]

Around 5 per cent of the global population is contemplating or undertaking migration at any time.[13] The number of people (foreign students, visitors and migrants) entering Australia is projected to increase significantly.[14]

Evidence is now suggesting, however, that globalisation is generating resistance. The worst global financial crisis since the 1930s[15], apparently unrestricted movements of people including workers and asylum-seekers, and the rise of violent extremism and terrorism[16] have led voters in many parts of the developed world to respond anxiously to some of globalisation's economic and social consequences.

Economic polarisation, evidenced in high levels of youth unemployment, homelessness and poverty, is casting an increasing number of young people into extremely vulnerable situations.[17] Social alienation and disaffection with a social system often lead to survival crime and public displays of defiance and resistance to authority.[18] The impact of this will be determined largely by the extent to which these conditions continue over the coming decades.

Transnational crime

Globalisation has brought many benefits, but it has also ushered in a step change in global risk.[19] Australia's place in the globalised economy exposes it to increasingly powerful transnational illicit activity.[20] The cost of involvement in transnational criminal activity is asymmetric to the effect such activity has on the economy. Approximately 70 per cent of Australia's serious and organised crime threats are based offshore or have offshore links.[21]

The impact of transnational crime on the economy

Organised crime is recognised as an issue of national security. Organised crime costs Australia in the order of US$36 billion annually.[22] It also causes great harm to individuals and the broader community. The UN Office of Drugs and Crime has estimated that criminals launder about 2.7 per cent of world GDP annually.[23] Cybercrime currently costs the global economy an estimated US$445 billion per annum.[24] It is likely to become one of the most prevalent and lucrative criminal activities in Australia.

From the Al-Qaeda attacks with aircraft in New York and Washington in 2001, to Daesh's sophisticated use of social media to radicalise individuals, terrorists have proven adept at using cutting-edge technology to communicate securely, publish propaganda, transfer funds and undertake reconnaissance securely and remotely.

The economic impact of global terrorism has been rising steadily since 2010. The Institute for Economics and Peace calculated its cost at more than $52 billion in 2014.[25] The 9/11 attacks were initially estimated to have cost $27.2 billion, but the inclusion of indirect and long-term expenditures brings the amount closer to $3.3 trillion.[26]

Interstate and intrastate conflict

Interstate and intrastate conflict with regional consequences and large-scale unregulated migration are among the top five most likely risks to global security.[27] More than 65 million people are now displaced worldwide due to persecution, conflict, generalised violence or human rights violations.[28]

Environmental impact

Environmental stresses are also contributing to global uncertainty. As carbon pollution pushes atmospheric greenhouse gases to the highest concentrations ever recorded,[29] more extreme weather events and natural disasters are likely, particularly in South Asia, East Asia and the Pacific[30]; where around half the world's major natural disasters occurred in 2014.[31] This is likely to lead to more frequent demands for humanitarian relief operations and to drive further migration and movement.

The global population is expected to reach 8 billion in 2025[32]. Rising numbers of people and expanding urbanisation will increase the contest for space and resources.[33] By 2030 the demand for food, water and energy will grow by approximately 35 per cent, 40 per cent and 50 per cent, respectively.[34] Almost half of the global population will live in areas of severe water stress.[35] Fragile states in Africa and the Middle East are at most risk of food and water shortages.[36] All of this is likely to drive further large-scale involuntary migration.[37]

Australia is a wealthy country, but its wealth, interests and viability are spread globally and depend strongly on international exposure.[38] As the Australian population grows to between 36 million and 48 million by 2061[39], more Australians will seek to live and invest offshore[40] and more of the world's people, goods, ideas and communications will reach Australia, either physically or through the internet.

Despite the emerging resistance to globalisation, the technologies that made it possible, and the new technologies discussed below, cannot be uninvented. States will remain the most important voice in international affairs, but the influence and capacity of non-state actors – ranging from private companies to terrorist groups – will grow, challenging the state in some areas.[41] The challenges that globalisation and its related technologies present to state sovereignty, traditional boundaries[42] and the business of policing will continue.

TECHNOLOGY DRIVERS – FUTURE DISRUPTION

Five fast-paced 'future technology trends – digitisation, connection, automation, material manipulation and augmentation – are emerging that have the potential to disrupt and reshape international society, crime and policing.

Experts estimate that by 2020, the digital universe will contain nearly as many digital bits as there are stars in the universe[43]

Digitisation

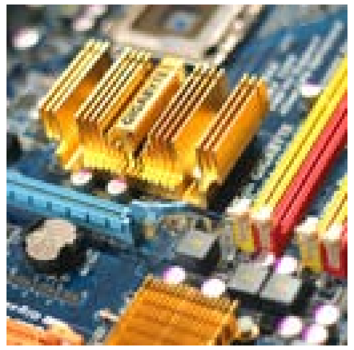
Digitisation is the conversion of an object, data or image into an electronic format. Its power is that it creates a common language. Data about ideas and behaviour can be stored, analysed and shared on a mass scale, just like data about the physical world. Money, legal contracts and the code of life itself (DNA) can all be digitised.

Digitisation lies behind the explosion in 'big data'. By 2020 there will be 10 times the amount of digitised information as there was in 2013.[43] This data explosion creates new types of value by helping organisations do everything from predicting buying behaviour to fighting crime. It is shifting the concept of value from physical and social assets to digital assets.[44]

'Why do you rob banks?' a journalist once asked the American criminal Willie Sutton. 'Because that's where the money is', he allegedly replied. Crime moves to where the value is. Criminal organisations are 'going digital' to capture value and financial profit. By leveraging data, they will be able to create new ways of capturing value at a previously unforeseen scale.[45] Their intention may be to steal, accrue, manipulate or delete data or hold it to ransom.

Connection

Connectivity means greater productivity, but also increased vulnerability.



The internet has changed the way humankind functions.[46] In its pervasiveness, the internet has altered the way people communicate and the way they form and develop relationships. It has redefined language, concepts of privacy and how people work, play and relax. It has changed the way they do business and exchange information, how they shop, bank and navigate and, importantly, how (and who, or what) they trust.[47]

There is no evidence to suggest that the development of the internet is slowing. Indeed, its geographical reach is expanding[48], thanks to 4G and 5G connections. Approximately half of the world's population are now connected to the internet[49]– most via their mobile phones.[50] It is estimated that by 2020, 90 per cent of all people over the age of six will have a mobile telephone.[51]

The IoT is the name given to the networking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enable them to collect and exchange data.[52] Potentially, every device, building and phone will be permanently connected to humans, to other devices and to the internet.[53]

The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems and offering improved efficiency, accuracy and economic benefit.[54] Industry experts estimate that the IoT will consist of almost 50 billion objects by 2020.[55] This world offers incredible opportunities, but also exposes society to increased vulnerabilities[56], many of which cannot yet be identified.[57]

The internet has made it easier for factories and other plants to automate operations using industrial control systems. Some sources, however, estimate that 92 per cent of such systems have known security vulnerabilities.

The future world will be more convenient and responsive to people's needs, but there will be a trade-off between convenience and the vulnerability of our connected devices[58], the dimensions of which we do not yet fully understand. Individual privacy will face unprecedented challenges[59] and protecting it will become a significant issue for individuals and governments.

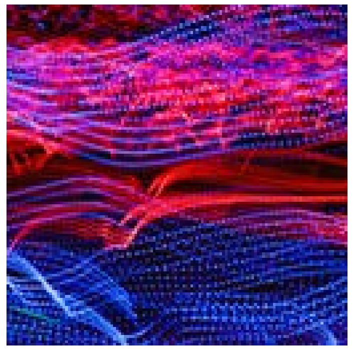
Connectivity is extending the geographical reach and scalability of crime.

The interconnectedness of digital communication and physical hardware is extending the reach of crime. Criminals around the world can collaborate securely online. Not only can they carry out new types of crime, but they can do so from a distance and at greater scale. One person armed with malware can commit a crime against millions of people in multiple jurisdictions. Criminals can search for the weakest link in a network of connections and then use it to access the wider network.

Encryption and the 'darknet' will result in crimes involving multiple systems, actors and technologies across jurisdictions. Next-generation devices with ESIM functionality (mobile devices with embedded inbuilt SIM cards) allow the end user to subscribe with one or more mobile virtual network operators, or physical network operators[60], typically located in a different country from the end user.[61] Commercial encryption and mobile virtual network operators will assist criminal global logistics by making the transnational movement of value and digitised goods difficult to detect.

Perhaps the most significant harm, including potentially to state revenue, may come from criminal use of alternative banking platforms and virtual currencies.[62] Distributed ledger technology (also known as 'blockchain'[63]) is likely to be highly disruptive to contemporary value transfer structures. It will transform the ability of criminals to move and hide their funds and digitised illicit goods[64], exacerbating the effects of globalisation on the state revenue base and making the burden of proof much heavier.

Automation



New kinds of physical and intellectual tasks are being performed by machines.

Improved power systems, new materials, advances in computing and manufacturing, and new, better algorithms are accelerating the development of robotics.[65] Robots are becoming faster, stronger, cheaper and more perceptive, allowing them to engage with their environments and carry out increasingly complex tasks. The value of the output of the global robotics industry is expected to surpass $151 billion by 2020.[66]

Associated with this is the development of artificial intelligence (AI), perhaps the single most revolutionary technology trend of the future. AI enables machines, through a combination of self-learning algorithms and computer systems, to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and language translation. Investment in AI start-ups has increased significantly in the last five years. Machines are rapidly challenging humans at learning, predicting and deciding.

In the same way that smartphones became widely available from 2006 onwards, robotics and AI will become cheap, easily accessible and deployable in the future.[67] People will be sharing their worlds with increasingly smart machines that have a form of limited or governed artificial intelligence, minimising human intervention in areas that were previously considered beyond automation – for example, driving a car, investing money or teaching in classrooms.

The introduction of autonomous and AI systems will, however, also give rise to complex new legal and ethical challenges.[68] Criminals will be quick to adopt automated technologies, which will test traditional policing approaches. Robotic systems will make it possible to conduct personless crime from remote locations, through an intermediary or via the internet. Anyone can download or buy pre-made malicious software packages online and get tips and DIY advice from underground websites or chat rooms; a single operator can carry out multiple, simultaneous attacks; a drone is capable of carrying an improvised explosive device; driverless cars can deliver bombs; an algorithm can set up phishing scams that steal banking information and then skim fractional amounts from millions of accounts so that it is unnoticeable.[69] In 2008 'hacktivists' copied and replicated the German Interior Minister's fingerprint, encouraging use to impersonate the minister on biometric readers.[70]

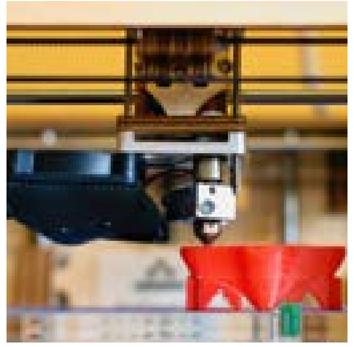
Predictions that automation will make humans redundant have been made many times, but going back to the Industrial Revolution technology has always ended up creating more new jobs than it destroys. However, the short- to middle-term disruption to society will always manifest and create challenges requiring policing and law enforcement responses.[71]

Material manipulation

Four technologies – digital manufacturing, nanotechnology, gene editing and synthetic biology – are enabling society to digitise, manipulate and reproduce nearly every aspect of the material and biological environment.

Digital manufacturing (also known as 3D printing) has rapidly advanced from producing cheap plastic gimmicks to enabling printing of almost any material[72], from carbon fibre[73] to marble[74] to human tissue.[75] New methods of 3D printing such as laser sintering[76] and stereo lithography[77] are dramatically improving the speed and accuracy of digital manufacturing. More powerful 3D scanning techniques allow for the capture of any object or scene in high fidelity, and new light field camera technologies[78] create entirely new possibilities for digital imaging. In the future, these technologies will be combined with advanced spectrometers to allow the reproduction of any object just by taking a picture of it.[79]

3D printing will enable the production of high-quality goods and no longer require complex global supply chains and economies of scale.[80] Greater productivity, shorter lead times, fewer supply chain risks and lower environmental and financial costs[81] will result.



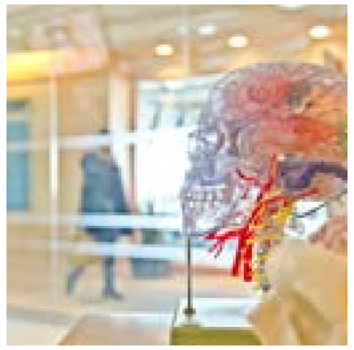
Nanotechnology may enable people to rearrange molecules with atomic precision. Similarly, alchemy could enable the creation of new compounds, giving materials new properties – from self-healing buildings[82] to tiny robots in the bloodstream.[83]

In the biological sciences , the last decade has seen the arrival of full genomic sequencing and, new techniques for gene editing that make it very simple to 'cut and paste' DNA.[84] It is already possible, to create semi-synthetic life forms[85] and alter existing ones such as crops[86] and viruses. These technologies will enable us to cure many diseases[87], extend lifespans[88] and improve overall health and quality of life.[89]

However, as the technologies of material manipulation mature, they will make possible new and more effectual types of crime. Advanced 3D manufacturing will enable criminal syndicates to manufacture products and bypass established regulatory frameworks. This potentially has significant implications for the protection of intellectual property[90] and taxation.[91]

The ability of criminals to manipulate physical objects, change molecular structures and genetics and edit DNA has the potential to undermine traditional forensic signatures.

Augmentation



Machines and humans are being linked up to bolster physical and mental capabilities. New capabilities will produce unpredictable and possibly profound shifts in society.

New forms of interaction between people and machines will become available. These include virtual reality[92], which enables users to immerse themselves in a digital environment; augmented reality[93], which overlays the real world with digital information and images; machine-to-brain interfacing[94], which enables people to manipulate computers and machinery with their minds; and new forms of biological[95] and chemical[96] enhancement, which aim to increase people's intellectual and physical capabilities.

Augmented reality, virtual reality and mixed reality represent the next major wave of computing.[97] That wave is coming quickly – there are already more than a million monthly users of virtual reality wearables.[98] As these technologies develop, they will allow for a seamless interface between the physical and digital worlds. According to experts, within 15 years the bulk of our work and play time will touch the virtual to some degree.[99] Systems for delivering these shared virtual experiences will become enormous enterprises, providing new mechanisms for people to connect with one another.

Mixed reality will be accompanied by other forms of augmentation. Brain-to-machine interfacing has already been used for transmitting thoughts across long distances[100], for controlling drones[101] and for moving robotic limbs.[102] Implantable devices, controlled by a neural interface, will be able to use chemical or neurostimulation to perform a wide range of tasks – from fighting diabetes[103] to firing a gun more effectively.[104] As the brain and body become increasingly blended with digital and physical technology, augmented communities of interest will begin to emerge in some parts of the world, with significant implications for security and privacy.[105]

As early adopters of technology, operating in an ethically unconstrained environment, criminals will be among the first to experiment with augmentation, permitting the creation of stronger, smarter and faster offenders.

IMPLICATIONS FOR THE AFP

SECTION 3

3

The increased complexity of the operating environment will place greater demands on the AFP's capabilities and will require the application of new types of skills.

Globalisation and advances in technology have moved economic and social activity well beyond single jurisdictions[106], providing criminals with much bigger pools of victims and the ability to undertake activities from foreign safe havens beyond the reach of local policing authorities. International criminal syndicates can collaborate on an unprecedented scale.[107] There are also signs that the strategies of some crime groups and state actors are beginning to align more closely, blurring the lines between organised crime and legitimate entities.[108]

Data and value can be accessed and transferred across multiple jurisdictions at the press of a button. Crime organisations will mirror big business in embracing digital innovation and will employ tools, analytics, programmers and hackers to capture value. The AFP will need to access and harness big data and develop an appropriately skilled workforce to combat future serious and organised criminality.

Traditional physical barriers such as borders, guards and gates have become increasingly difficult to make less permeable. As passenger volumes increase and facilities expand, the demand for AFP services at major Australian airports and other establishments is likely to grow.[109]

The calls on AFP resources to assist the development of policing in Australia's nearby region are also likely to continue. Policing expertise and community engagement will be increasingly important in helping to manage instability in many regional countries.[110] Climate change and more intense weather patterns will disproportionately affect fragile states in Asia and the Pacific[111], leading to likely requirements for AFP contributions to humanitarian assistance and disaster relief.

The AFP will need to continue to develop its operational capabilities against those wishing to disrupt the Australian way of life, working in close collaboration with state and territory police, the intelligence community and international law enforcement partners. The trend towards unheralded violent acts using commonplace weapons perpetrated by unknown individuals, or those who have been assessed as low risk, is likely to continue alongside more sophisticated attacks.[112]

> Faster, more agile crimes demanding faster, more agile responses

Given the complexity of the future operating environment, demand will continue to outstrip the AFP's capacity. Everything new the AFP does will come at an opportunity cost to existing commitments.

The AFP will need to become a more technologically capable organisation, with more effective strategic planning and the flexibility to allocate resources to rapidly evolving specialist technologies. It will need to be able to respond to and disrupt new types of crime in an environment of increasing complexity and uncertainty.

Criminals will be able to perpetrate crimes, such as child abuse (including the active targeting of vulnerable children via anonymised use of the internet and virtual currencies), theft or sexual assault[113] in virtual environments. They will continue to use malware (including ransomware) for a range of criminal purposes, from the creation of fake login screens[114] for banking apps, to holding victims to ransom by blocking access to a computer system until a sum of money is paid.[115] The AFP will need to adapt its current practices to maintain an effective presence in this virtual criminal environment.

Technological developments will greatly reduce the time frames for police to deal with crime. At the same time, matters that could previously be resolved by the work of a small number of detectives will increasingly require the application of specialist capabilities in areas such as cyber, forensic accounting, law, intelligence analysis, technical interception and surveillance across multiple jurisdictions. These capabilities have traditionally been reserved for matters of only the highest priority. More emphasis will need to be placed at the point of referral with the application of intelligence-informed targeting and processes.

The use of multidisciplinary and multi-agency teams, comprising detectives and specialist investigative capabilities, to resolve standard investigations will become the norm. This will require a recalibration of the AFP's existing workforce and greater public sector partnerships.

The AFP will have to rely more heavily on external experts from the private sector, other government agencies and the research community to help identify supply chain dependencies and exploitation risks and develop ways of mitigating them. Private sector partnerships will require new approaches to reform some traditional practices, such as engaging with industry to jointly develop more efficient ways to achieve all required security clearances and meet engagement requirements. The AFP will also need to undertake broader engagement with international partners to support global efforts to respond to cybercrime.

The AFP's strategic workforce plan will need to reflect the requirement for a diverse, inclusive, ethical, skilled and experienced workforce, with higher levels of technical expertise in fields such as cybercrime and intellectual property offences. It will also need to provide the tools to support them.

Recruitment will have to be geared towards multiple entries from apprentice to graduate pathways. New generations will enter the workforce who are more likely to seek 'out of portfolio' careers, rejecting traditional models of lifelong service with one employer[116] and testing the traditional model of recruitment, in which police officers and subject matter experts are trained in-house over many years.

As criminals develop unanticipated new methods, the AFP will have to be able to generate new capabilities and expertise through strategies such as filling more temporary positions with independent workers for short-term contracts.

The evolution of technology and the criminal and terrorism threat environment over the next five to 10 years will test the boundaries of existing legislation. It will be essential that the legislative framework under which the AFP works keeps pace with the rate of change. The effectiveness of global legal frameworks, which are focused primarily on nation-states, will be challenged as more and more evidence lies offshore.[117] Further, as its reliance on traditional DNA and biometric evidence is tested, the AFP will need to research new, more secure identification techniques such as brain scanning and microbiome analysis.[118]

The AFP should assume a greater leadership role in the delivery of national investigative standards and training curricula for its Commonwealth law enforcement partners. The establishment of an investigations training and accreditation centre of excellence could deliver national investigative standards and training curricula for all Commonwealth law enforcement agencies. Such a centre could establish capability benchmarks for the standard of investigations, and drive continuous improvement by sharing capabilities and experiences. It would help generate a common understanding of techniques and investigative tools, including technology, harmonise the interpretation of legislation, ensure better information-sharing and help strengthen the personal networks of law enforcement professionals.

```
a.fn.scrollspy=d,this},a(w
y),+function(a){"use strict
e[b]()})}var c=function(b)
ropdown-menu)"),d=b.data("t
st a"),f=a.Event("hide.bs.t
faultPrevented()){var h=a(d
rigger({type:"shown.bs.tab
i > .active").removeClass("
```

THE WAY FORWARD

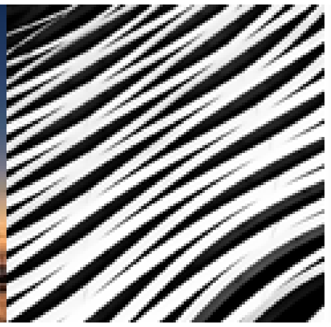
SECTION 4

Globalisation of world trade, financial services, transport networks, people movements and economic activity are challenging the single jurisdictional view of law enforcement. Increased connectivity and awareness are also driving expectations from government and the community for faster turnaround and response times by agencies. The complexity of this landscape is affecting the AFP in terms of its areas of focus and the way in which it balances these demands with an appropriate response.

To be successful, the AFP will need to adopt a more robust approach to understanding requirements and then developing and deploying its unique capabilities.

The AFP has already begun preparing for the future by modifying its organisational structure. In July 2015, it moved to a new operational, capability and capacity-based model.

To realise its strategy for future capability, the AFP will develop and implement a capability framework comprising four strategic capabilities: policing, law enforcement, people and asset protection (incorporating critical infrastructure), and international engagement.



AFP CAPABILITY FRAMEWORK

In ordinary usage, 'capability' means the power to do or affect something. The term can refer to an ability, capacity or quality. In the AFP context, capability is the power to achieve a desired operational outcome or effect in a nominated environment, within a specified time and to sustain that effect for a designated period.

Policing

Policing protects life and property, prevents crime, detects and apprehends offenders, maintains order and helps those in need of assistance. The ultimate effect of good policing is the achievement of voluntary compliance with the law in the community.

Law enforcement

Law enforcement provides criminal investigations, case management and operational response elements focused on organised crime and gangs, cybercrime and cyber safety, child protection, countering terrorism and violent extremism, and the associated recovery of the proceeds of crime.

People & asset protection

People and asset protection provides protection services for senior politicians, visiting dignitaries and diplomats, witnesses and associated sites of critical importance. It also provides counter-terrorism first response and undertakes firearms and explosive detection searches.

International engagement

International engagement provides international policing cooperation, liaison, international stabilisation, capacity-building and policing assistance aligned with Australia's national interests.

The AFP will deliver against these four strategic capabilities through the use of multidisciplinary teams comprising sworn members, professional staff and industry partners. To keep Australia safe, the AFP will pursue strategies that are designed primarily to prevent and disrupt crime. It will do this by enhancing policing partnerships globally and nationally to create a hostile environment for criminals.

FUTURE AREAS OF FOCUS

To develop these four capabilities for the future, the AFP will pursue a raft of activities, with particular focus on:

Intelligence-informed targeting and processes

The AFP will be intelligence-informed, agile and adaptive. The AFP's intelligence-informed triage and prioritisation processes will be critical to ensuring that finite resources are assigned to greatest effect.

Transnational serious and organised crime

Consistent with the priority of combatting national security threats, the focus of AFP investigative activity will be on complex transnational serious and organised crime, including violent extremism. In combatting organised crime, the AFP will provide the interface between national security and domestic policing issues.

The most tangible criminal threat to Australia's national security is terrorism and this threat will continue for the foreseeable future. Well-planned and coordinated attacks are probable, as is the likelihood of more attacks emanating from unknown individuals using unsophisticated means.

The AFP, in collaboration with state and territory police, the intelligence community, law enforcement agencies and international partners, will continue its role in safeguarding Australia's national security at home and offshore. As a key agency in the Australia – New Zealand Counter Terrorism Committee, the AFP will work with state and territory police to ensure effective preparedness for, prevention of, responses to and recovery from terrorism incidents.[119]

Prosecutorial action will remain a primary deterrent; however, harm-reduction strategies will become increasingly important and will require a greater application of regulatory action and prevention and disruption approaches, domestically and internationally. Effective harm-minimisation requires a whole-of-government approach to which the AFP will be a major contributor.

Within this environment the AFP will continue to adopt an investigative partnership approach, working collaboratively with and drawing on the strengths and capabilities of different agencies, public and private, domestic and international. This approach provides layers of depth to create a preventative shield from crime for Australia and its people.

National and international leadership and coordination

The AFP has a well-deserved reputation for its ability to effectively coordinate and facilitate partnerships with diverse agencies, in both the public and private sectors, across national and international jurisdictions.

The AFP will coordinate multijurisdictional operational activity through its national and international network of offices and people.

The AFP plays a critical coordination role through its leadership of national and international joint taskforces targeting transnational serious and organised crime.

Leveraging the AFP's abilities in facilitating and leading partnership arrangements will help to maximise successful operational outcomes, nationally and internationally.

International engagement

The AFP will be the principal international representative for Australian policing and law enforcement.

The AFP is recognised nationally and internationally as a strong and credible international policing leader. The AFP provides its policing and law enforcement partners with a critical capacity to extend investigations offshore and conduct overseas inquiries on a police-to-police basis. The AFP will lead and conduct international operations on behalf of all Australian state, territory and Commonwealth policing and law enforcement agencies.

The AFP will continue to place significant emphasis on its international presence, working with international partners to combat crime at its source and disrupt criminal networks and avert security threats in Australia. The AFP will be the primary Australian representative for many international policing initiatives, such as the Pacific Islands Chiefs of Police Forum, the Chiefs of ASEAN Police Forum, INTERPOL and the Virtual Global Taskforce to combat online child sexual abuse.

These international relationships will also form an integral component of broader government efforts to strengthen regional and international partnerships, including by supporting regional security, stability and peacekeeping. The AFP will provide the Australian Government with deployable international policing capabilities that enable it to deliver immediate stability operations, short-term emergency responses and long-term regional police development.

Technical and niche proficiencies

The AFP will develop unique proficiencies and exploit advanced technologies that support Australia's national interest. To this end, the AFP will engage leading-edge specialist technicians to provide expertise for the AFP and the broader Australian policing and law enforcement community.

Knowledge will be critical to the way the AFP defines threats, directs resources, delivers prioritised services to government and the community and informs strategic thinking. Investment in contemporary technology and capability solutions will be crucial to enable the effective management of information critical to defining and countering threats to the Australian national interest.

The AFP requires an integrated information environment, characterised by enterprise-level data pooling and powerful analytics, underpinned by modern technology infrastructure that is capable of sustained management of high volumes of data. Integrated components will provide the AFP with seamless access to, and analysis of, large datasets in real time to identify changing dynamics and mitigate national security threats.

The AFP will seek to:

- develop and maintain capabilities at a pace consistent with that of the security threat and criminal environment
- establish a framework to determine which capabilities it will develop and hold in-house and which it will outsource
- lead in developing technical and specialist capabilities that can be shared with and utilised by state, territory and Commonwealth partners
- partner with the private sector to develop solutions for the future
- move its culture from a functional perspective that applies traditional policing models to one where specialist skills are engaged early to define problems and help resolve them.

AFP as knowledge leader

The AFP's operating environment is shaped by policy and legislative frameworks. Accordingly, informed and effective policy and legislation has a direct deterrence and disruptive effect. As the Australian Government's primary adviser on policing issues, the AFP will work closely with the federal Attorney-General's Department to identify ways in which emerging technology and changing criminal behaviour challenge the boundaries of existing legislation. The AFP will continue to ensure that any changes to the powers of the AFP and other law enforcement agencies are proportional, appropriate and effective.

The AFP will pursue a greater leadership role in the delivery of national investigative standards and training curricula across a range of its technical and niche proficiencies for both national and international law enforcement partners.

The AFP's future workforce

In the future, organisational success will be increasingly dependent on how well a diversity of views and expertise are harnessed to innovate, adapt and effect change.

To be future-ready and be an employer of choice, the AFP will continue to build an ethical, values-driven culture that embraces diversity, inclusion and mutual respect. Doing so will attract and retain a gender-inclusive, culturally and ethnically diverse workforce reflective of Australian society. This will include people from Aboriginal and Torres Strait Islander backgrounds, people with disability and people with diverse gender identity and sexual orientation.

The AFP will develop a flexible, collaborative and multi-skilled workforce comprising individuals of high integrity who are capable of critical thinking, reflection, analysis and independent judgement.

The future AFP workforce will be characterised by different engagement models and partnerships, a higher proportion of technical and specialist skills and an enhanced qualifications framework to ensure the best resources are applied to solve existing and emerging problems.

The AFP will value partnerships with academia to inform organisational learning and research-based reform.

Future AFP leaders will be highly adaptive, value the views and expertise of others, communicate effectively, speak the languages of policing and technology, and embrace ethical conduct and values that reflect the society they serve.[120]

The AFP will undertake its functions in a manner that respects human rights and freedoms as they apply to all people: in training its staff, in building capacity of other police services, in its compliance with international conventions and in the execution of its remit.

The AFP will invest in technically focused capabilities, working with industry and the research community.

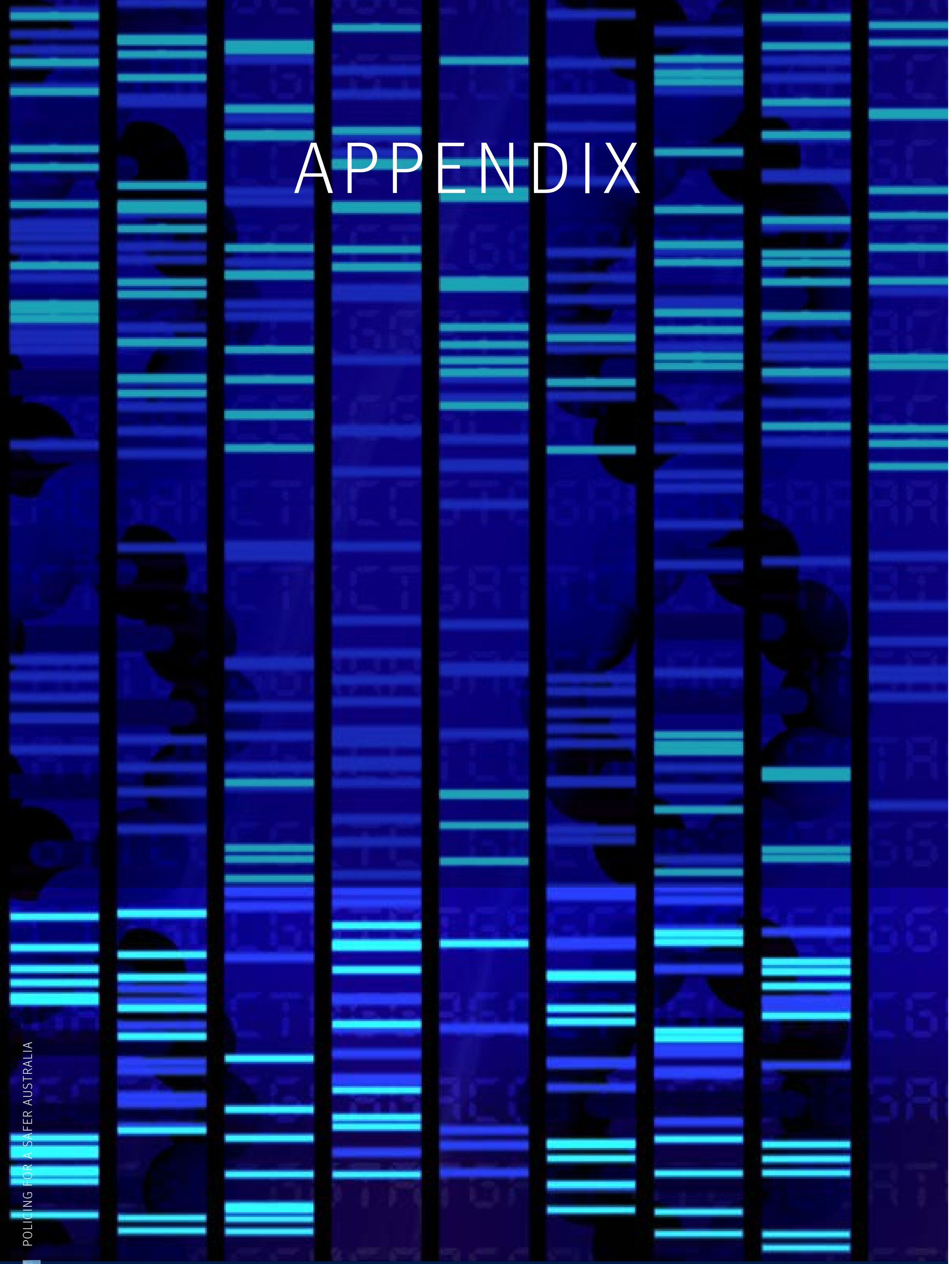
Measuring success

The test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with them[121]. An enduring challenge for the AFP is that traditional performance measurements cannot adequately capture the effectiveness of preventative and disruptive measures to mitigate community harms. Future success will need to be measured not only quantitatively but qualitatively, based on the effective deterrence and disruption of crime impacting Australian interests.

CONCLUSION

As a result of this appreciation of the drivers of the future of criminality impacting Australian interests, and through the careful delivery of these and other activities, the AFP is now honing its focus to achieve maximum effect against the known challenges and threats and those not yet realised.

APPENDIX



PROCESS

The AFP launched its Future Directions project to explore the future of the AFP in a speech delivered by the Commissioner to the Lowy Institute for International Policy in March 2015.[122]

An expert advisory board provided high-level direction and experience across the fields of policing, government, national security, economics, international affairs and human rights. Its members were:

- Chief Commissioner Graham Ashton, Victoria Police
- Sir Angus Houston, Special Envoy in relation to MH17 and former Chief of the Defence Force
- Mr Warwick Jones, Executive Director of the Australian Institute of Police Management
- Dr Martin Parkinson, Secretary of the Department of the Prime Minister and Cabinet
- Dr Helen Szoke, Chief Executive Officer of Oxfam
- Professor Michael Wesley, Director of the Coral Bell School of Asia Pacific Affairs at the Australian National University.

The Future Directions Strategic Context Paper launched in July 2015 asked: What should the Australian Federal Police look like, 15 years from now? This question formed the basis for conversations with staff and with the AFP's national and international partners across law enforcement, intelligence, police, government and academia.

The key themes identified by stakeholders included:

- the need for the AFP to better define its identity
- the uniqueness of the AFP, given its local, national and international remit
- the need for the AFP to prioritise its operational effort in light of finite resources
- the need to preserve and develop the AFP's expertise in dealing with complex serious organised crime and national security matters
- the critical national importance of the AFP's international collaboration in the broad national security and law enforcement context
- the importance of the AFP's role in providing leadership and coordination on serious organised crime investigations and matters impacting Australia's national security
- the need for the AFP to add value to the work of partner agencies by providing unique specialist capabilities.

This paper has also been informed by a wide range of literature, reports, statistics and commentary, and has explored work being undertaken within the AFP to ensure that the outcomes of the strategy are embedded in future changes across the organisation.

Alignment will be achieved through a series of implementation plans being developed by the accountable teams within the organisation to work towards practice and process improvements. These plans will deliver outcomes across the AFP workforce learning and education, technology, information and intelligence, and international engagement to deliver long-term transformational change.

GLOSSARY

3D printing	A process that begins with the virtual design of an object using a 3D modelling program. The object is then created by laying down successive layers of material. Each of these layers can be seen as a thinly sliced horizontal cross-section of the eventual object.
3D scanning	Scanning via an imaging device that collects distance point measurements from a real-world object and translates them into a virtual 3D object.
artificial intelligence	Enables machines, through a combination of self-learning algorithms and computer systems, to perform tasks normally requiring human intelligence, like visual perception, speech recognition, decision-making and language translation.
augmentation	The linking of machines and humans to increase human physical and mental capabilities. It includes virtual reality, augmented reality, machine-to-brain interfacing, and new forms of biological enhancement and chemical enhancement.
augmented reality	A form of augmentation technology that overlays the real world with digital information and images.
automation	The ability to automate physical and intellectual tasks via robotics or artificial intelligence.
big data	Datasets whose size is beyond the ability of typical software tools to capture, store, manage and analyse. Predictive analytics or other innovative methods may be required to extract value from data. Accuracy in big data can lead to better decision-making, resulting in greater operational efficiency, cost reduction and reduced risk.
blockchain	Distributed electronic ledger that uses software algorithms to record and confirm transactions with reliability and anonymity. The record of events is shared between many parties, and information once entered cannot be altered because the downstream chain reinforces upstream transactions. It is the world's first technology capable of creating public, tamper-proof digital ledgers.
brain scanning	Scanning that maps the brain's neuronal pathways and relates the connectivity patterns to personality and behaviour.

connectivity	Enables connection of anything and everyone, anywhere. Almost half of the world's population, 3.3 billion people, are connected to the internet, most via mobile phones.
Cybercrime	Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide. Although there is no single universal definition, law enforcement generally makes a distinction between two main types of internet-related crime: • advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software • cyber-enabled crime – many traditional crimes have taken a new turn with the advent of the internet, such as crimes against children, financial crimes and even terrorism
digital communication	The physical or electronic transfer of digitally encoded data. Data transmitted may originate from a digital data source like a computer or keyboard, or from an analogue source (e.g. from a phone call or video signal).
digital manufacturing	A process that uses 3D visualisation, analytics and simulation to simultaneously create and manufacture a product. It allows engineers to create the entire manufacturing process in a virtual environment, incorporating feedback from production operations in the design process.
digitisation	The transformation of information about the world into a common digital language in the form of binary code. It turns information into a common, global resource that can be shared on a massive scale.
fragile state	A country in which the government has limited capacity, or will, to provide basic services and security to its citizens and the relationship between the government and its citizens is weak. These states lack the institutions needed to resolve conflict peacefully.
gene editing	Insertion, deletion or replacement of DNA in the genome of an organism using engineered nucleases, or 'molecular scissors'.

brain to machine interfacing	A form of augmentation technology that enables people to manipulate computers and machinery with their minds.
malware	Software that is specifically designed to disrupt or damage a computer system.
megacity	A city with 10 million or more occupants.
microbiome analysis	The study of microbial communities found in and on the body. The goal of microbiome studies is to understand the role of microbes in health and disease.
nanotechnology	Manipulation of matter on an atomic, molecular and supramolecular scale. It involves the ability to see and control individual atoms and molecules.
physical hardware	The physical parts or components of a computer system.
phishing scam	A form of internet fraud in which an email purporting to be from a legitimate sender encourages the recipient to provide personal information ostensibly to confirm or update legitimate information which the legitimate organisation already has.
robotics	The branch of mechanical engineering, electrical engineering and computer science that deals with the design, construction, operation and application of robots, as well as computer systems for their control, sensory feedback and information processing.
sintering	To bring about the agglomeration of particles of a metal or other substance by heating, usually under pressure.
stereo lithography	The process of printing a multidimensional image.
synthetic biology	An emerging scientific field in which engineering principles are utilised to design and assemble biological components, biological systems and machines for useful purposes.
virtual reality	A form of augmentation technology that enables users to immerse themselves in a digital environment.
wearables	Clothing and accessories incorporating computer and advanced electronic technologies.

NOTES

1. Patten, C. (1999). *A new beginning: Policing in Northern Ireland – Report of the Independent Commission on Policing for Northern Ireland*. [online] Belfast: Independent Commission on Policing in Northern Ireland, p. 18. Available at: http://cain.ulst.ac.uk/issues/police/patten/patten99.pdf.

2. Section 8 of the *Australian Federal Police Act 1979* (the AFP Act).

3. Section 37(2) of the AFP Act.

4. Australian Federal Police (2014). *Ministerial direction*. [online] Available at: https://www.afp.gov.au/about-us/governance-and-accountability/governance-framework/ministerial-direction.

5. Economist.com. (2012). *A fall to cheer.* [online] Available at: http://www.economist.com/node/21548963.

6. Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K. and Dhingra, D. (2016). *Digital globalization: The new era of global flows.* [online] McKinsey & Company. Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

7. Humanorigins.si.edu (2016). *Humans change the world*. Smithsonian Institution. [online] Available at: http://humanorigins.si.edu/human-characteristics/humans-change-world.

8. United Nations (2014). *World's population increasingly urban with more than half living in urban areas*. [online] Available at: http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html.

9. Department of Infrastructure and Regional Development (2015). *State of Australian cities 2014–2015*. Canberra: Department of Infrastructure and Regional Development.

10. UK Government (2014). *Global strategic trends out to 2045*. 5th edn. Swindon: UK Ministry of Defence. Available at: https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045.

11. United Nations Department of Economic and Social Affairs Population Division (2015). *International migration report 2015*. [online] Available at: http://www.un.org/en/development/desa/population/migration/publications/migrationreport/docs/MigrationReport2015_Highlights.pdf.

12. World Economic Forum (2016). *The global risks report 2016*. 11th edn. [online] Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

13. United Nations Department of Economic and Social Affairs Population Division (2013). *The number of international migrants worldwide reaches 232 million*. Population facts. [online] United Nations. Available at: https://esa.un.org/unmigration/documents/the_number_of_international_migrants.pdf.

14. Australian Border Force (2016). ABF 2020. Canberra: Australian Border Force.

15. Domitrovic, B. (2013). The worst economic crisis since when? [online] Forbes.com. Available at: http://www.forbes.com/sites/briandomitrovic/2013/02/05/the-worst-economic-crisis-since-when/#6b595edd34a7.

16. US Agency for International Development (2011). *The development response to violent extremism and insurgency*. US Agency for International Development.

17. Australian Youth Policy and Action Coalition (1992). *Federal budget submission – Australian Youth Policy & Action Coalition* Inc. Canberra: The Coalition.

18. White, R. (1989). Making ends meet: young people, work and the criminal economy. *Australian and New Zealand Journal of Criminology,* vol. 22, no. 3, pp. 136–50. Available at: http://journals.sagepub.com/doi/abs/10.1177/000486588902200302;White, R. 1990, *No space of their own: Young people and social control in Australia*. Melbourne: Cambridge University Press.

19. Committee for Development Policy (2000). *Economic globalization: trends, risks and risk prevention.* CDP background paper no. 1. [online] United Nations Development Policy and Analysis Division, Department of Economic and Social Affairs. Available at: http://www.un.org/en/development/desa/policy/cdp/cdp_background_papers/bp2000_1.pdf.

20. Office of National Assessments (2016). *Strategic illicit threats into harm's way.* Canberra: Office of National Assessments.

21. Australian Criminal Intelligence Commission (2016). *Criminal syndicates.* [online] Available at: https://www.acic.gov.au/about-crime/organised-crime-groups/criminal-syndicates.

22. Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism (2015). *Serious and organised crime costing Australia $36 billion*. [online] Available at: https://www.ministerjustice.gov.au/Mediareleases/Pages/2015/FourthQuarter/18-December-2015-Serious-and-organised-crime-costing-Australia-36-billion.aspx.

23. United Nations Office on Drugs and Crime (2011). *Illicit money: how much is out there?* [online] Available at: https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html.

24. World Economic Forum (2015). *Global risks 2015*. Insight report. [online] World Economic Forum, p. 6. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf

25. Holmes, F. (2016). *The global cost of terrorism is at an all-time high.* [online] Businessinsider.com. Available at: http://www.businessinsider.com/global-cost-of-terrorism-at-all-time-high-2016-3?IR=T.

26. Carter, S. and Cox, A. (2011). One 9/11 tally: $3.3 trillion. *New York Times.* [online] Available at: http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0.

27. World Economic Forum (2016). *The global risks report 2016.* 11th edn. [online] Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

28. UNHCR (2015). *Forced displacement in 2015*. Global trends. [online] UN Refugee Agency. Available at: http://www.unhcr.org/statistics/unhcrstats/576408cd7/unhcr-global-trends-2015.html.

29. Guardian (2014). *Greenhouse gas emissions rise at fastest rate for 30 years.* [online] Available at: https://www.theguardian.com/environment/2014/sep/09/carbon-dioxide-emissions-greenhouse-gases.

30. World Economic Forum (2016). T*he global risks report 2016*. 11th edn. [online] Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

31. United Nations Economic and Social Commission for Asia and the Pacific (2015). *Enhanced regional cooperation key to building resilience to floods and landslides*. [online] Available at: http://www.unescap.org/news/enhanced-regional-cooperation-key-building-resilience-floods-and-landslides.

32. United Nations Sustainable Development (2015). *UN projects world population to reach 8.5 billion by 2030, driven by growth in developing countries.* [online] Available at: http://www.un.org/sustainabledevelopment/blog/2015/07/un-projects-world-population-to-reach-8-5-billion-by-2030-driven-by-growth-in-developing-countries.

33. World Economic Forum (2016). *The global risks report 2016*. 11th edn. [online] Geneva: World Economic Forum. Available at: http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.

34. Office of the Director of National Intelligence (2016). *Global trends 2030*: *Alternative worlds*. National Intelligence Council.

35. UN.org (2016). *Water scarcity – International Decade for Action 'Water for Life' 2005–2015*. [online] Available at: http://www.un.org/waterforlifedecade/scarcity.shtml.

36. Office of the Director of National Intelligence (2016). *Global trends 2030: Alternative worlds*. National Intelligence Council.

37. World Economic Forum (2015). *The global risks report 2015*. 10th edn. [online] Geneva: World Economic Forum. Available at: http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/introduction.

38. Wotherspoon Wealth (2015). *5 reasons to go global.* [online] Available at: https://wotherspoonwealth.com.au/5-reasons-to-go-global.

39. Australian Bureau of Statistics (2015). *3222.0 – Population projections, Australia, 2012 (base) to 2101.* [online] Available at: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/3222.0main+features52012%20(base)%20to%202101.

40. Lu Yueyang, M. (2016). Super funds to invest in offshore property. *The Australian.* [online] Available at: http://www.theaustralian.com.au/business/property/super-funds-to-invest-in-offshore-property/news-story/14efed88523b0417ee9bc74847411a1c.

41. UK Government (2014). *Global Strategic Trends out to 2045*. 5th edn. Swindon: UK Ministry of Defence. Available at: https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045.

42. Ip, E. (2010). Globalization and the future of the law of the sovereign state. *International Journal of Constitutional Law,* vol. 8, no. 3, pp. 636–55. Available at: http://icon.oxfordjournals.org/content/8/3/636.full.

43. Emc.com (2014). *Executive summary: Data growth, business opportunities, and the IT imperatives – The digital universe of opportunities: rich data and the increasing value of the Internet of Things.* [online] Available at: http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

44. Deloitte (2016). *The value shift: Why CFOs should lead the charge in the digital age.* [online] Available at: http://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-digital-age-business-model-innovation-value.html.

45. Secureworks.com (2016). *5 tactics cyber criminals use to capture personal & financial data.* [online] Available at: https://www.secureworks.com/blog/cyber-criminal-tactics.

46. Naughton, J. (2010). *The internet: Is it changing the way we think?* [online] *The Guardian*. Available at: https://www.theguardian.com/technology/2010/aug/15/internet-brain-neuroscience-debate.

47. Edge (2010). 2010: *How is the internet changing the way you think?* [online] Available at: https://www.edge.org/responses/how-is-the-internet-changing-the-way-you-think.

48. Simonite, T. (2016). *Google's loon balloons are ready to deliver cheap internet.* [online] *MIT Technology Review.* Available at: https://www.technologyreview.com/s/534986/project-loon.

49. Internetlivestats.com (2016). *Number of internet users (2016) – Internet Live Stats.* [online] Available at: http://www.internetlivestats.com/internet-users.

50. Benedict Evans (2016). *The end of a mobile wave; the Dell of mobile.* [online] Available at: http://ben-evans.com/benedictevans/2016/4/29/the-end-of-a-mobile-wave.

51. Ericsson.com (2014); *Ericsson Mobility Report: percent will have a mobile phone by 2010* [online]. Available at: https://www.ericsson.com/news/1872291

52. Morgan, J. (2014). *A simple explanation of 'the internet of things'.* [online] Forbes.com. Available at: http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5166261c6828.

53. McLellan, C. (2016). *M2M and the Internet of Things: A guide.* [online] ZDNet. Available at: http://www.zdnet.com/article/m2m-and-the-internet-of-things-a-guide.

54. Morgan, J. (2014). *A simple explanation of 'the internet of things'.* [online] Forbes.com. Available at: http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5166261c6828.

55. Getgds.com (2016). *Internet of things solutions from global data systems.* [online] Available at: http://www.getgds.com/internetofthings.

56. Internet of Business (2016). *Beware trade off IOT convenience security.* [online] Available at: http://www.internetofbusiness.co.uk/insight/2016/01/28/beware-trade-off-iot-convenience-security.

57. USA.kaspersky.com (2016). *Kaspersky lab discovers vulnerable industrial control systems likely belonging to large organizations.* [online] Available at: http://usa.kaspersky.com/about-us/press-center/press-releases/2016/Kaspersky-Lab-Discovers-Vulnerable-Industrial-Control-Systems-Likely-Belonging-to-Large-Organizations.

58. Internet of Business (2016). *Beware trade off IOT convenience security.* [online] Available at: http://www.internetofbusiness.co.uk/insight/2016/01/28/beware-trade-off-iot-convenience-security.

59. Rainie, L. and Anderson, J. (2014). *The future of privacy.* [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewinternet.org/2014/12/18/future-of-privacy.

60. Meukel, M., Schwarz, M. and Winter, M. (2016). *E-SIM for consumers – a game changer in mobile telecommunications?* [online] McKinsey & Company. Available at: http://www.mckinsey.com/industries/telecommunications/our-insights/e-sim-for-consumers-a-game-changer-in-mobile-telecommunications.

61. KPMG (2016). *Jumping on the MVNO brandwagon: How niche can you get?* [online] Available at: http://kpmg.com.au/portals/0/9266-mvnowhitepaper-jan06.pdf.

62. Pflaum, I. and Hateley, E. (2014). *A bit of a problem: national and extraterritorial regulation of virtual currency in the age of financial disintermediation.* 1st edn. Washington: Georgetown.

63. Bravenewcoin (2016). *Bravenewcoin: Blockchain an 'essential' tech for CEOs, states PwC.* [online] Steemit.com. Available at: https://steemit.com/money/@bravenewcoin/bravenewcoin-blockchain-an-essential-tech-for-ceos-states-pwc.

64. Mihm, S. (2013). *Are bitcoins the criminal's best friend?* [online] Bloomberg View. Available at: https://www.bloomberg.com/view/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-.

65. Berman, A. (2016). *These five exponential trends are accelerating robotics.* [online] Singularity HUB. Available at: http://singularityhub.com/2016/05/11/five-exponential-trends-are-accelerating-robotics.

66. Tractica (2015). *Global robotics industry to surpass $151 billion by 2020.* [online] Tractica.com. Available at: https://www.tractica.com/newsroom/press-releases/global-robotics-industry-to-surpass-151-billion-by-2020.

67. Waters, R. and Bradshaw, T. (2016). *Rise of the robots is sparking an investment boom.* [online] *Financial Times.* Available at: http://www.ft.com/cms/s/2/5a352264-0e26-11e6-ad80-67655613c2d6.html#axzz4J4SDHaQS.

68. Etzioni, O. and Etzioni, A. (2016). *Designing AI systems that obey our laws and values.* [online] Cacm.acm.org. Available at: http://cacm.acm.org/magazines/2016/9/206255-designing-ai-systems-that-obey-our-laws-and-values/fulltext.

69. Stross, R. (2010). $9 here, 20 cents there and a credit-card lawsuit. *New York Times.* [online] Available at: http://www.nytimes.com/2010/08/22/business/22digi.html?_r=1.

70. Zetter, K. (2008). *Hackers publish German minister's fingerprint.* [online] WIRED. Available at: https://www.wired.com/2008/03/hackers-publish.

71. Economist.com (2016). *The impact on jobs – Automation and anxiety: Will smarter machines cause mass unemployment.* Special report, 25 June. Available at: http://www.economist.com/news/special-report/21700758-will-smarter-machines-cause-mass-unemployment-automation-and-anxiety.

72. Murphy, M. (2016). *We're closer to a future where we can 3D print anything.* [online] Quartz. Available at: http://qz.com/654180/were-closer-to-a-future-where-we-can-3d-print-anything.

73. 3ders.org (2016). *The strongest players in carbon fiber 3D printing today.* [online] Available at: http://www.3ders.org/articles/20160229-the-strongest-players-in-carbon-fiber-3d-printing-today.html.

74. Sher, D. (2015). *3D printing helps robotic marble sculptors push the limits of digital manufacturing.* [online] 3dprintingindustry.com. Available at: http://3dprintingindustry.com/news/3d-printing-helps-robotic-marble-sculptors-push-limits-digital-manufacturing-51763.

75. abc.net.au (2016). *3D printing breakthrough produces functioning human-scale bone and muscle tissue.* [online] Available at: http://www.abc.net.au/news/2016-02-18/3d-printing-breakthrough-enables-human-sized-functioning-tissues/7178800.

76. Williams, H. (2016). *An Australian company has achieved a world-first in 3D printing.* [online] Gizmodo.com.au. Available at: http://www.gizmodo.com.au/2016/05/an-australian-company-has-achieved-a-world-first-in-3d-printing.

77. 3ders.org (2016). *Stereolithography (SLA) viable for making 3D printed pills, recent study shows.* [online] Available at: http://www.3ders.org/articles/20160418-stereolithography-sla-viable-for-making-3d-printed-pills-recent-study-shows.html.

78. Koo, R. (2016). *Watch lytro change cinematography forever.* [online] No Film School. Available at: http://nofilmschool.com/2016/04/lytro-cinema-camera-cinematography-demo?goal=0_aa18ea5b4e-f598131561-284370133.

79. Temperton, J. (2015). *This quantum dot spectrometer fits on your smartphone.* [online] WIRED UK. Available at: http://www.wired.co.uk/article/quantum-dot-spectrometer-breakthrough.

80. Mohr, S. and Khan, O. (2015). 3D printing and its disruptive impacts on supply chains of the future. *Technology Innovation Management Review*, [online] vol. 5, no. 11. Available at: http://timreview.ca/article/942.

81. Hervey, A. (2015). *How 3D printing could transform a $20 billion industry.* [online] Backchannel. Available at: https://backchannel.com/how-one-australian-entrepreneur-is-about-to-disrupt-a-20-billion-industry-you-ve-never-heard-of-254afd0269e8.

82. Prodromakis, T. (2016). Nanotechnology is changing everything from medicine to self-healing buildings. *Independent.* [online] Available at: http://Nanotechnology is changing everything from medicine to self-healing buildings.

83. American Chemical Society (2015). *Toward nanorobots that swim through blood to deliver drugs* (video). [online] Available at: http://www.eurekalert.org/pub_releases/2015-06/acs-tnt061715.php.

84. Ledford, H. (2016). CRISPR: gene editing is just the beginning. *Nature News*, [online] vol. 531, no. 7593, p. 156. Available at: http://www.nature.com/news/crispr-gene-editing-is-just-the-beginning-1.19510.

85. Pollack, A. (2016). Scientists talk privately about creating a synthetic human genome. *New York Times*. [online] Available at: http://www.nytimes.com/2016/05/14/science/synthetic-human-genome.html?_r=1.

86. Ledford, H. (2016). Gene-editing surges as US rethinks regulations. *Nature News*, [online] vol. 532, no. 7598, p.158. Available at: http://www.nature.com/news/gene-editing-surges-as-us-rethinks-regulations-1.19724.

87. Trafton, A. (2016). Curing disease by repairing faulty genes. [online] *MIT News*. Available at: http://news.mit.edu/2016/crispr-curing-disease-repairing-faulty-genes-0201.

88. Bioviva-science.com (2016). *First gene therapy successful against human aging*. Blog. [online] Available at: http://www.bioviva-science.com/blog/first-gene-therapy-successful-against-human-aging-2.

89. Trafton, A. (2016). *Curing disease by repairing faulty genes*. [online] MIT News. Available at: http://news.mit.edu/2016/crispr-curing-disease-repairing-faulty-genes-0201.

90. Gartner (2013). *Gartner reveals top predictions for IT organizations and users for 2014 and beyond*. [online] Available at: http://www.gartner.com/newsroom/id/2603215.

91. Flynn, C. (2015). *3D printing taxation issues and impacts*. [online] ey.com. Available at: http://www.ey.com/Publication/vwLUAssets/ey-3d-printing-taxation-issues-and-impacts/$FILE/ey-3d-printing-issues-impacts.pdf.

92. Strauss, K. (2016). *Virtual reality jobs jump in the job market*. [online] Forbes.com. Available at: http://www.forbes.com/forbes/welcome/?toURL=http://www.forbes.com/sites/ karstenstrauss/2016/05/11/virtual-reality-jobs-jump-in-the-job-market/&refURL=&referrer=%20-%2029ac2b0a4e19.

93. Kelly, K. (2016). *The untold story of Magic Leap, the world's most secretive startup*. [online] WIRED. Available at: http://www.wired.com/2016/04/magic-leap-vr.

94. Murphy, M. (2015). T*his mind-controlled prosthetic robot arm lets you actually feel what it touches*. [online] Quartz. Available at: http://qz.com/500572/this-mind-controlled-prosthetic-robot-arm-lets-you-actually-feel-what-it-touches.

95. Darpa.mil (2015). *Work begins to support self-healing of body and mind*. [online] Available at: http://www.darpa.mil/news-events/2015-10-05.

96. Dance, A. (2015). *Smart drugs: A dose of intelligence*. [online] Nature.com. Available at: http://www.nature.com/nature/journal/v531/n7592_supp/full/531S2a.html.

97. Dixon, C. (2016). *What's next in computing?* Blog. Available at: https://medium.com/software-is-eating-the-world/what-s-next-in-computing-e54b870b80cc.

98. Samsung AU. (2016). *Gear VR*. [online] Available at: http://www.samsung.com/au/consumer/mobile-phone/wearables/gear/SM-R322NZWAXSA.

99. Kelly, K. (2016). T*he untold story of Magic Leap, the world's most secretive startup*. [online] WIRED. Available at: http://www.wired.com/2016/04/magic-leap-vr.

100. Iozzio, C. (2016). *Scientists prove that telepathic communication is within reach*. [online] Smithsonian. Available at: http://www.smithsonianmag.com/innovation/scientists-prove-that-telepathic-communication-is-within-reach-180952868/?no-ist.

101. ABC News (2016). *Mind-controlled drone race a first for techno brain power at University of Florida*. [online] Available at: http://www.abc.net.au/news/2016-04-27/mind-controlled-drone-race-florida/7362172.

102. BBC.com (2016). *The teen who made a revolutionary robot arm*. [online] Available at: http://www.bbc.com/future/story/20151026-a-teens-mind-controlled-arm-could-make-prosthetics-cheaper.

103. Financial Times (2016). *Monitor implant approved for UK diabetics*. [online] Available at: http://www.ft.com/cms/s/af8251b0-d186-11e5-92a1-c5e23ef99c77,Authorised=false.html?siteedition=intl&_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2Faf8251b0-d186-11e5-92a1-c5e23ef99c77.html%3Fsiteedition%3Dintl&_i_referer=http%3A%2F%2Fsearch.ft.com%2Fsearch%3FqueryText%3Dmonitor%2Bimplant&classification=conditional_standard&iab=barrier-app#axzz4JR21ronA.

104. Radiolab (2014). *9-volt nirvana*. [online] Available at: http://www.radiolab.org/story/9-volt-nirvana.

105. WIRED (2016). *Wearables and quantified self demand security-first design*. [online] WIRED. Available at: http://www.wired.com/insights/2014/10/wearables-security-first-design.

106. Imf.org (2016). *Issues brief – Globalization: A brief overview*. [online] Available at: https://www.imf.org/external/np/exr/ib/2008/053008.htm.

107. Elliott, L. (2016). Fourth Industrial Revolution brings promise and peril for humanity. *Guardian*. [online] Available at: https://www.theguardian.com/business/economics-blog/2016/jan/24/4th-industrial-revolution-brings-promise-and-peril-for-humanity-technology-davos.

108. Cockayne, J. (2016). *Hidden power: Organised crime in international politics*. [online] Australian Institute of International Affairs. Available at: http://www.internationalaffairs.org.au/australian_outlook/hidden-power-organised-crime-in-international-politics.

109. Australian Border Force (2016). *ABF 2020*. Canberra: Australian Border Force; Westernsydneyairport.gov.au (2016). Western Sydney Airport. [online] Available at: http://westernsydneyairport.gov.au.

110. UN Police Division (2014), *Strategic guidance framework for international police peacekeeping*, p. 3.

111. World Economic Forum (2015). *The global risks report 2015*. 10th edn. [online] Geneva: World Economic Forum. Available at: http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/introduction.

112. Management Systems International (2009). *Guide to the drivers of violent extremism*. [online] United States Agency for International Development. Available at: http://pdf.usaid.gov/pdf_docs/Pnadt978.pdf.

113. Sipress, A. (2007). Does virtual reality need a sheriff? *Washington Post*. [online] Available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/06/01/AR2007060102671.html.

114. Taha, M. (2016). *Android users under attack from new malware targeting major banks*.

115. Heater, B. (2016). *The growing threat of ransomware*. [online] PCMag Australia. Available at: http://au.pcmag.com/security/42855/news/the-growing-threat-of-ransomware.

116. PwC (2011). *Millennials at work – Reshaping the workplace*. [online] Available at: https://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/assets/reshaping-the-workplace.pdf.

117. Michaels, R. (2016). *Globalization and law: Law beyond the state*. [online] Durham: Duke University. Available at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5540&context=faculty_scholarship.

118. Pollack, A. (2009). DNA evidence can be fabricated, scientists show. *New York Times*. [online] Available at: http://www.nytimes.com/2009/08/18/science/18dna.html?_r=0.

119. Australia-New Zealand Counter-Terrorism Committee. *Australian National Security*. [online] Available at: https://www.nationalsecurity.gov.au/WhatAustraliaisdoing/Pages/Australia-New-Zealand-Counter-Terrorism-Committee.aspx.

120. Herrington, V. and Colvin, A. (2016). Police leadership for complex times. *Policing*, [online] vol. 10, no. 1, pp. 7–16. Available at: http://policing.oxfordjournals.org/content/10/1/7.full?sid=c39566cb-153f-4d6a-987e-04841e0a6755.

121. Mark, R. (1978). *Report to the Minister for Administrative Services on the organisation of police resources in the Commonwealth area and other related matters*. Canberra: Australian Government Publishing Service, p. 28 and Appendix F.

122. Colvin, A. (2015). *Lowy Lecture Series*. Lowy Institute for International Policy, 5 March, Sydney.

AFP
AUSTRALIAN FEDERAL POLICE

POLICING FOR
A SAFER AUSTRALIA

AFP
AUSTRALIAN FEDERAL POLICE

POLICING FOR
A SAFER AUSTRALIA