SPECIAL REPORT

ASPI

I can see clearly now!

Technological innovation in Australian law enforcement:
A case study of anti-money laundering

Dr John Coyne and Amelia Meurant-Tompkinson

July 2018

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

About the authors

Dr John Coyne joined ASPI as the Senior Analyst for the Border Security Program in February 2015. John comes to ASPI from the Australian Federal Police, where he worked on transnational serious organised crime, national security and counterterrorism. Over the past 20 years, he has been an intelligence professional at tactical, operational and strategic levels in a range of military, regulatory, national security and law enforcement organisations. During that period, he has worked extensively in the ASEAN region, delivering a range of bilateral research projects. His more recent work in this area has focused on enhancing multilateral ASEAN information exchange regarding non-traditional illicit commodity flows. John's border security research interests include intelligence, private–public sector cooperation in the border environment and the integration of border security operations.

Amelia Meurant-Tompkinson is an ASPI Research Intern. She was awarded the university medal for her honours thesis, which examined the role of hydropolitics in the Turkish-Kurdish conflict. Prior to joining ASPI, Amelia has five years' experience in human rights and public diplomacy across government and non-government, most recently monitoring the referendum in Iraqi Kurdistan. Her current research interests focus on geopolitics in the MENA region, human security and statebuilding.

Acknowledgement

This report finds its origins in conversations between ASPI and Oracle staff on law enforcement innovation. At the time, Oracle wanted to make a contribution to Australian public policy dialogue on technology innovation in law enforcement. From these conversations Oracle kindly provided ASPI corporate sponsorship for an innovation research project. ASPI would like to acknowledge Oracle's support for this project, without which this report would not have been possible.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Graphic of assorted Australian currency. Photo: Ryan Fletcher/Alamy Stock Photo.

I can see clearly now!

Technological innovation in Australian law enforcement: A case study of anti-money laundering

Dr John Coyne and Amelia Meurant-Tompkinson

July 2018

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

First published July 2018

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

EXECUTIVE SUMMARY

The Australian Government's technological monopolies have ended. Technological developments, especially those that have been disruptive, have been driven primarily by private corporations for at least the past 10 years. Meanwhile, legislative responses to those changes, be they disruptive or otherwise, have been increasingly delayed, the current state of the *Telecommunications (Interception and Access) Act 1979* (Cwlth) being a case in point.[1]

Acceleration in the development and use of technology has been matched by changes in the capability of those who would do us harm. In the face of rapid social change, governments have lost more than a technological edge, as the very conceptualisations of sovereignty and geographical jurisdictions are being challenged. Law enforcement agencies' traditional business models for dealing with organised crime are under significant pressure from threat actors that are able to operate more agile decision-making cycles and exploit seams between jurisdictions and in law enforcement agencies' capabilities.

In this context, Australian law enforcement agencies face an increasing number of challenges from emergent technologies. A key policy challenge underpinning these issues relates to the limited capacity of law enforcement to introduce innovative[2] strategies in response to disruptive technology. Another is how to make cross-jurisdictional cooperation simpler and easier.

The complexity of responding to the technological innovation challenge isn't lost on law enforcement or the Australian Government. In 2018, the Parliamentary Joint Committee on Law Enforcement commenced an inquiry into the 'Impact of new and emerging information and communications technology'.[3]

Our research explored technological innovation in law enforcement through a specific crime type case study of anti-money laundering (AML) provisions. One of the most effective disruption strategies available to law enforcement is the innovative use of AML provisions to disrupt access to funds by non-state actors (organised crime and terrorist groups).

This report analyses the factors that support or restrict technological innovation in federal law enforcement's AML efforts. While this research focused on technology and AML, it has broader application to technological innovation in law enforcement.

The report argues that the current ecosystem for technological innovation for AML needs to be enhanced to engage with the dual challenge of disruptive technology and the integration of existing pockets of AML excellence into a holistic whole-of-government innovation program. The initial steps for responding to this challenge should include an analysis of the central assumptions that underpin innovation, policymaking, strategy and finance in this space.

Innovators and strategists alike need to be mindful that predictive analytics aren't a panacea for random events or the unknowable future. It's unlikely that such analytics will foresee inflection points beyond the data used to construct models.

It seems almost certain that future technological innovation will largely be done by industry, not government, although governments can be drivers of innovation by investing in science and technology and by setting challenges for industry that innovation can solve. The private sector's perspective is that this reality is having lasting impacts on public sector technological innovation, and so strategic partnerships with the private sector need to become the norm.

Law enforcement innovation agendas, especially for AML, face a plurality of organisational and cultural challenges. Among them, this research identifies three core issues: innovation cultures, innovation focus, and innovation integration.

The evidence seems clear that communities and nations will experience increasingly more frequent technological disruptions that will revolutionise our way of life. While those disruptions will appear outside of conventional thinking, they will then be rapidly accepted and normalised. Engaging with such new thinking, new opportunities, new risks and new threats requires cultures of innovation in enforcement and regulatory agencies.

Our research found little evidence that the organisational frameworks for enterprise or portfolio technological innovation in federal law enforcement are fully developed. Furthermore, despite the existence of various pockets of innovation excellence in Australia's law enforcement community, there were indicators of cognitive bias in some of the thinking on technological innovation. In many cases, there was a symmetry in agency responses that could also be evidence of the need for more contested policy perspectives and advice.

Overall, this research revealed that the focus of technological innovation in AML is often on specific platforms, tools and capabilities at the expense of more strategic thinking.

Cumulatively, innovation in AML is often more akin to a cottage industry. Technological innovation integration isn't being widely considered. Therefore, technologies aren't consistently well integrated into organisational strategies, across portfolios, or across the whole of government.

However, by no means does this report argue that technological innovation isn't occurring, or that agencies don't have the right people. Rather, the law enforcement sector has the time and capability for a disruptive change of its own. The key to this disruption won't be innovation theatre, but a far more tangible change and commitment to realising those changes.

PURPOSE

Law enforcement agencies' traditional business models for dealing with organised crime are under significant pressure from threat actors that are able to operate more agile decision-making cycles. One of the most effective disruption strategies available to law enforcement involves using anti-money laundering (AML) provisions innovatively to disrupt access to funds by non-state actors (organised crime and terrorist groups).

However, proactively identifying deviant or anomalous flows of funds is increasingly difficult. When it comes to AML, before a matter can even be referred to law enforcement for investigation, private and public compliance and regulatory systems must be able to identify—with a high degree of accuracy—deviant or anomalous behaviour. As Australia's compliance responses to AML evolve in response to this challenge, financial sector compliance arrangements have also become complex.

The operational sophistication and technological capabilities of organised crime today have made AML investigations increasingly complicated. While law enforcement's regulatory and compliance data analytic capabilities are continuously improving, they're still struggling with the storage and analysis of growing datasets, let alone the widespread application of emergent technologies such as artificial intelligence or self-learning algorithms.

The complexity of responding to the technological innovation challenge isn't lost on law enforcement or the Australian Government. In 2018, the Parliamentary Joint Committee on Law Enforcement commenced an inquiry into the 'Impact of new and emerging information and communications technology'. In response, and with generous financial support from Oracle, this research project sought to explore technological innovation in law enforcement through a specific crime type case study.

This paper analyses the key factors that support or restrict technological innovation in federal law enforcement AML efforts. While this research was focused on technology and AML, it has broader application to law enforcement technological innovation.

This research project was underpinned by three key questions:

1. How can technology enhance the identification of money laundering offences?
2. How can law enforcement bring together technology and policy to ensure more agile AML decision-making?
3. How can law enforcement agencies gain faster access to new AML technologies and capabilities?

The report's central argument is that the current ecosystem for technological innovation in AML needs to be enhanced to engage with the dual challenge of disruptive technology and the integration of pockets of AML excellence into a holistic whole-of-government program. The initial steps for responding to this challenge should include an analysis of the central assumptions that underpin innovation, policymaking, strategy and finance in this space.

BACKGROUND: THE LAW ENFORCEMENT TECHNOLOGICAL INNOVATION CHALLENGE

At the turn of the millennium, cutting-edge computing capability was still being driven by governments. However, the speed at which technology has been developed and then deployed has since accelerated exponentially. In the process, the Australian Government's technological monopolies have ended. There's no binary answer to whether this is a positive or negative development; rather, it's a truism of the contemporary environment that policymakers face.

More recently, technological developments, especially those that have been disruptive, have subsequently been driven predominantly by private corporations. Legislative responses to those changes, disruptive or otherwise, have been increasingly delayed. In some cases, the corporations responsible for the changes draw their research and development (R&D) budgets from revenues that exceed those of some governments. Complex ownership, financial and geographical arrangements make it difficult for governments to regulate these companies. However, the rising disruptive influence of small enterprises and start-ups has shown that at least some of this change isn't just about available finance but about entrepreneurial approaches to technological innovation. In this space, 'innovation' refers to industrialising the generation of new approaches.

Governments haven't had a significant independent technological edge for many years. Instead, in the past their advantage was created by companies in sectors dependent on government spending—notably defence. This situation has shifted now so that innovation is coming from commercial sectors that aren't primarily driven by government investment. Regardless, in the face of this rapid change, governments have lost more than a technological edge. The very conceptualisations of sovereignty and geographical jurisdictions are being challenged.

By the early 2000s, our day-to-day life was mostly viewed by policymakers through two conceptual lenses: real and virtual. Government's policy responses to technology, at least in Australia, treated technological challenges through similarly divided silos. In the meantime, events such as the launch of the iPhone in 2007 by Steve Jobs were altering the way that many of us interact with each other and the world. Today, many Australians are unlikely to see their life or social interactions as divided between the real and the virtual: it's just their life.

Unsurprisingly, technological disruptions to the way our world operates are becoming more frequent and potent. For those in government, many of our underlying policy assumptions about crime and security are now also being affected.

Acceleration in the development and use of technology has been matched by changes in the capability of those who would do us harm. State and non-state actors alike are actively leveraging technology to communicate, undertake information operations and conduct cyberattacks; for instance, the Islamic State terror group uses Twitter and Twitter bots to organise and market its message broadly.

Australian law enforcement agencies face an increasing number of challenges from emergent technologies. For ease of consideration, it's possible to categorise those challenges into four broad thematic groupings:

- the implications of specific technological developments
- encryption
- the continued globalisation of organised crime
- the declining impact of traditional policing responses.

A key policy challenge that underpins the issues facing the government relates more to the limited capacity of law enforcement, whether in Australia or in other countries, to introduce innovative strategies in response to disruptive technology.

Many parts of law enforcement are rapidly changing and becoming more global, but that doesn't mean an end to investigations and response roles. With the rising threat to domestic security from non-state actors, law enforcement agencies face a broad family of threats that are increasingly untouchable using extant police capabilities and legislative powers. The range of transnational untouchables—those which exploit the vulnerabilities of international legal regimes, safe havens and corruption—is increasing.

The ability of law enforcement to collect admissible evidence and prosecute emergent transnational non-state actors is limited by legal jurisdictions. While criminal organisations can cross a border in seconds, the collection of evidence from a foreign jurisdiction using mutual legal assistance treaty arrangements, where they exist, can take weeks or months. While a non-state actor can operate from anywhere at any time, our law enforcement agencies' operational freedom of movement is limited by the geographical borders established in domestic and international law.

This point is illustrated by the 2017 Sydney airline terrorist plot. In late July 2017, the Australian Federal Police (AFP) uncovered a suspected Islamic State plot to blow up an Etihad flight to Abu Dhabi. The terror group allegedly coordinated in Syria and mailed a bomb kit from Turkey. The kit was then collected by an alleged terror cell in Sydney. While this example shows that there are plenty of seams in non-state actors' activities that can be identified and exploited, disrupting transnational threats using law enforcement methodologies is challenging, even with the support of another country.

The detection of transnational criminals is becoming increasingly difficult. In a physical sense, proactively identifying deviant financial transactions, people and cargo across borders is being made ever more difficult by the exponentially growing number of legitimate transactions. This is making investigations more complex and time consuming, due in part to the increased sophistication and technological capabilities of criminal conspiracies but also to the density of cross-border flows.

Global supply chains and complex business structures are also making evidence collection more difficult. While data analytic capabilities are increasing, law enforcement is faced with growing information flows that are difficult to store and analyse. This point isn't lost on Australian law enforcement officials and policymakers, who know that at least part of the solution is broader adoption of new approaches such as data analytics.

The news isn't all bad when it comes to Australian law enforcement responses: there are pockets of excellence and consistent efforts for innovation. While most of the government's law enforcement efforts are focused on arrests and seizures, a very small yet extremely successful number of enforcement officers are focused on the disruption of threats—especially organised crime—using soft power, such as capacity development.

The impact of new and emerging information and communications technology (ICT) ensures that technological disruptions will increase rapidly. The implications of the current trajectory of technological developments is that the lifecycle of ICT investments will be drastically reduced, particularly when it comes to applications that run over the underlying ICT infrastructure of servers, networks and storage. So, while the AFP's current case management system might be decades old, the next one won't have the same usable life.

Law enforcement has traditionally employed a ‘grow your own’ approach to subject matter expertise and capability development. In the current operating context, it will need to engage more frequently to acquire capabilities and subject matter expertise on an as-required, contracted basis.

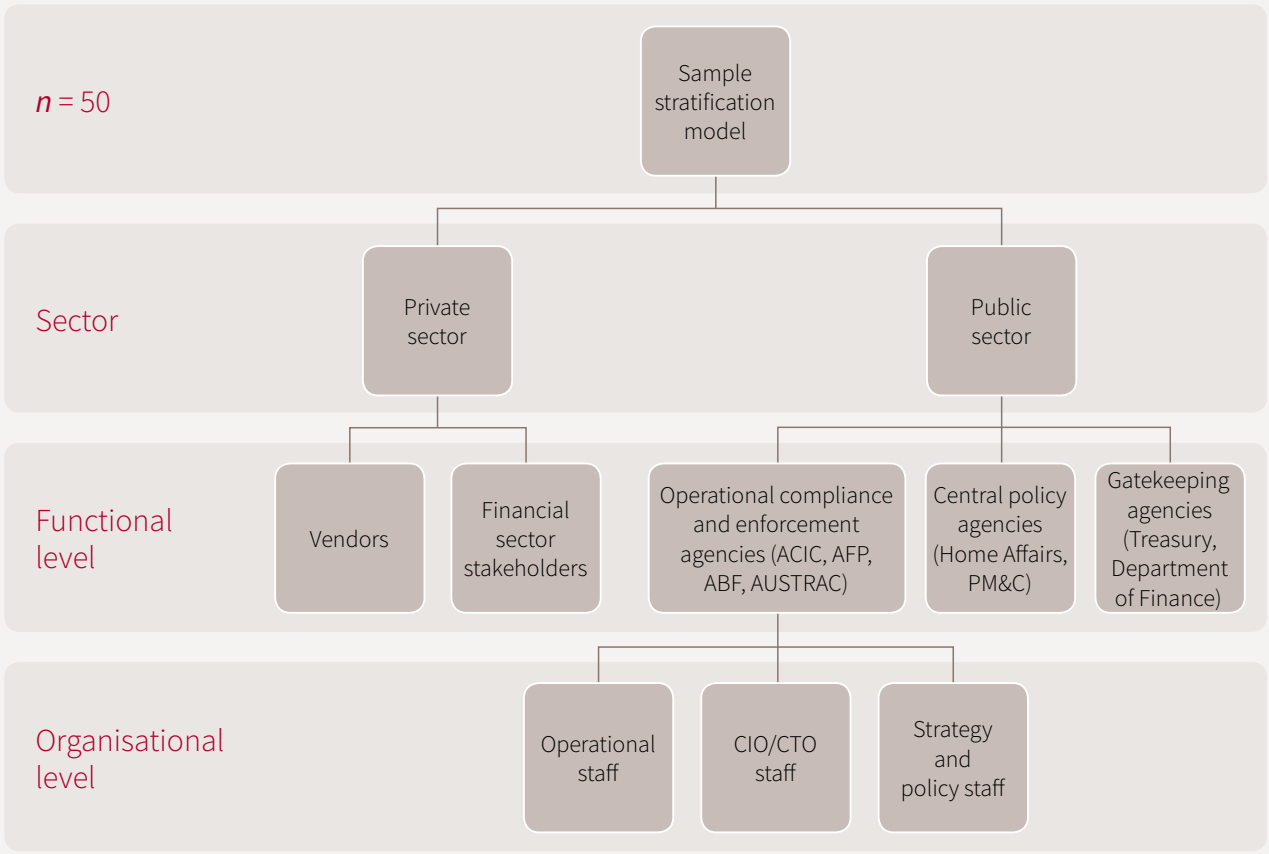
R&D budgets for law enforcement, especially for the development and rapid fielding of technological capabilities, need to drastically increase. While government is unlikely to be the predominant spender or regain its ‘technological edge’ as a quasi-monopoly customer, it can innovate and it can use its funding to drive private innovation that it can use. After all, law enforcement innovation is a broad term with organisational, cultural, finance and policy dimensions.

METHODOLOGY

Our research was underpinned by a mixed-methods qualitative research methodology using a specific case study of technological innovation in AML. Phase 1 of the research project involved undertaking a literature review. Phase 2 followed with the conduct of some 50 semistructured interviews with operational, strategic and enabling stakeholders from a range of private- and public-sector organisations, including vendors, financial-sector entities, the Department of Home Affairs, the Australian Border Force (ABF), the AFP, Treasury, the Australian Crime Commission, the Department of Finance and the Australian National Audit Office.

A purposive sampling methodology was used to select interview participants. Figure 1 provides a graphical representation of the sample stratification.

Figure 1: Sample stratification



AUSTRALIA'S AML REGIME

The beginnings of Australia's AML and counter-terrorism financing (CTF) regime came with the entry into force of the *Financial Transaction Reports Act 1988* (Cwlth). The Act was established to respond to the increasing profile of drug trafficking, a largely cash-based system, by legislating reporting on certain cash thresholds and establishing the Australian Transaction Reports and Analysis Centre (AUSTRAC).[4] Those measures were supplemented by stipulations on money laundering and terrorist financing offences in the *Criminal Code Act 1995* (Cwlth) and the *Proceeds of Crime Act 2002* (Cwlth).

Internationally, Australia has ratified the four foundational AML instruments:

- the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)
- the UN Convention for the Suppression of Financing of Terrorism (1999)
- the UN Convention against Transnational Organized Crime (2000)
- the UN Convention on Corruption (2003).

In 1989, Australia was a founding member of the Financial Action Task Force (FATF). The FATF is an intergovernmental body that sets out and assesses standards of legal, regulatory and operational measures for combating money laundering and terrorist financing.

The inaugural FATF *Mutual evaluation assessment* on the Australian AML regime, released on 14 October 2005, prompted a hefty transformation of the AML regime. The evaluation found that Australia's existing regime was noncompliant with approximately half of the FATF's 40 recommendations on money laundering.[5] In response, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth) (the AML/CTF Act) rapidly entered into force to address those shortcomings.

The Act forms the backbone of Australia's AML regime by setting out a system of reporting obligations on financial institutions. Those obligations include the identification and verification of customers, registering with AUSTRAC, reporting suspicious transactions and maintaining financial records for a minimum of seven years.[6]

While the AML/CTF Act is robust by international standards, the origins of the regime in cash-based transactions made it ill-prepared for the emergence of cryptocurrencies.[7] Until mid-2017, the Act defined 'e-currency' to be:

- an internet-based, electronic means of exchange that is backed either directly or indirectly by precious metal, bullion or a thing prescribed by the AML/CTF Rules and is not issued by or under the authority of a government body.[8]

That definition excluded digital currencies, such as Bitcoin, that don't have any physical 'thing' backing them. The oversight of digital currencies was a serious omission from the Act: Bitcoin has surpassed 85% of the total market capitalisation of digital currencies and poses various AML/CTF risks, given its anonymity and operation outside regulated financial systems.[9]

An amendment to the Act was passed in mid-2017, replacing 'e-currency' with 'digital currency' to bring an additional range of cryptocurrencies under its remit.[10] The increasing quantity and complexity of financial flows suggests that challenges will persist, and the law will have to innovate to keep up.

To address the rapidly changing financial environment, the AML/CTF Act conceptually consolidates a risk-based approach to AML.[11] The risk-based approach recognises that the financial institution is best placed to identify and assess the risks its business faces, and to develop controls and allocate resources that are proportionate to those risks. This approach thus provides scope for reporting entities and financial institutions to proactively seek out areas that could be problems. However, that hasn't always occurred. As an example, in June 2018, the Commonwealth Bank agreed to pay a $700 million fine, plus legal costs, for breaching AML provisions resulting in 'millions of dollars flowing through to drug importers'.[12]

The opportunity to implement the risk-based approach—that is, to proactively identify risks and implement AML measures at the financial institution level—remains hindered by limited national law enforcement resources. The most recent FATF *Mutual evaluation report*, released in 2015, found that authorities focus more on addressing predicate crimes ('the type of criminal conduct that generates funds which can then be laundered') than on money laundering.[13] The report commented that, overall, Australia doesn't have a developed national policy setting out what the AML regime is meant to achieve, or how its success should be monitored or measured, making it challenging for a risk-based approach to be effective.[14] Prioritising AML matters in national security is hence a crucial undertaking for an effective risk-based regime in future.

THE LAW ENFORCEMENT TECHNOLOGICAL INNOVATION CHALLENGE IN AML

The 'Fourth Industrial Revolution' is characterised as comprising a range of technological breakthroughs that are bringing together the physical, digital and biological worlds. This revolution is profoundly affecting law enforcement and security. While law enforcement is trying to look over the horizon at these challenges, it's faced with wrestling with more immediate innovation challenges. This is especially true for AML, in which regulators and law enforcement face a complex so-called 'big data' challenge.

Within the AML space, law enforcement is faced by five key innovation challenges:

1. How are we to identify suspect transactions or transaction patterns?
2. How, in this 'big data' environment, are we to collect information in an evidentiary form?
3. How are we to work across agency, jurisdictional, sectoral and geographical borders and boundaries?
4. How are we to increase the speed at which law enforcement is able to innovate in response to changes in the operating context?
5. How are we to increase the speed at which we're able to access new technologies?

These challenges are made more difficult by issues such as:

- the demise of the effectiveness of telephone intercepts due to encryption
- the further globalisation of crime and the declining impact of traditional policing responses
- organised crime groups that are often able to access new technologies and exploit vulnerabilities much quicker than their law enforcement counterparts can
- the quantity of financial transaction data, which is rapidly expanding while law enforcement's ability to match and mine that data is not developing with sufficient speed to meet this challenge.

OBSERVATIONS

The research methodology provided a descriptive dataset that offers an ethnographic perspective of innovation in AML law enforcement in Australia. However, presenting the research findings in an ethnographic format would not have provided readers with a sufficiently granular understanding of the dimensions of the applied policy challenge of technological innovation in AML. Accordingly, the following sections provide an explorative analysis of the key thematic research observations and their policy implications.

Key technologies

When it came to identifying the key technologies needed by Australian law enforcement to deal with money laundering, there were some startling differences in opinion over specific requirements among vendors, the public sector and the finance sector. This was particularly evident in R&D priorities.

The participating vendors were concerned with developing discovery and big-data analytics capabilities. In contrast, many of the public-sector research participants had a more operational focus on tools that will provide direct support to current AML investigations. Also in contrast, feedback from finance industry participants was more concerned with the Australian Government enhancing the availability of algorithms and intelligence that would make their existing systems work better, as opposed to specific technological solutions.

Public-sector research participants also had a different perspective on key AML technologies from the various Australian Government agencies that make up the Home Affairs AML enforcement community: the AFP, the Australian Criminal Intelligence Commission (ACIC), the ABF, AUSTRAC and the Home Affairs Department. The most startling difference of opinions on key technologies was found within, and across, the various federal agencies involved in investigations (the ACIC, AFP and ABF). While AFP operational staff did not clearly articulate their specific future technological needs, the ABF's operational staff argued that they sought to drive their innovation process by a bottom-up focus on specific proprietary products. Predictably, at the enterprise level, the ABF, AFP, ACIC and Home Affairs talked to the priority of information management and knowledge discovery.

Analysis revealed the following broad technological requirements identified by research participants:[15]

1. **Establishment of a big-data ecosystem.** While 'cloud', 'big data' and 'machine learning' have become buzzwords, there have been very real and meaningful advances in each of those technology sets outside of law enforcement. Many of the research participants talked of the need for these technologies. Those who were more technically minded broadened the requirement to include the need for combined technology stacks, in which capabilities and tools are developed in an ecosystem rather than in a series of individual programs.
2. **Content extraction and mapping.** Modern tools and platforms are needed to collate and process an exponentially expanding variety and volume of information. More specifically, law enforcement needs automated content extraction tools that collect information as objects, can analyse relations between objects and can present them in a manner that can be used both to support investigations and to assess the risk of deviance.

3. **Information enrichment.** Data ingested into law enforcement indices needs to be able to be further refined, either manually by human analysis or automatically using such capabilities as artificial intelligence, machine learning or natural language processing engines. Arguably, government needs to be able to create capabilities that can identify any concept inside text or objects. Those concepts need to be automatically stored and connected with similar objects inside data repositories.
4. **Multimedia pipeline.** Text needs to be able to be extracted from audio, video and image files using multimedia processing, with a combination of optical character recognition, speech-to-text and image object detection. This needs to be supported by natural language processing engines that automatically extract relevant AML information.
5. **Natural language processing and information classification.** There's a need for tools that extract information automatically from raw text, most document formats, images, audio files and videos. This capability needs to be able to identify such unique identifiers as names, organisations, geographical locations, email addresses, financial transfers and phone numbers. It also needs to be able to identify the sentiment of a given piece of text. It should group information into distinct categories based on thematic characteristics, using both statistical models and dictionaries from a variety of languages and dialects.
6. **Spatial analysis.** Information that holds geographical data should be able to be displayed and manipulated.
7. **Link analysis.** While law enforcers have been operating link analysis tools for almost two decades, the utility of those tools needs to be substantially increased. Law enforcement agencies need software, and the associated algorithms, for information processing that can be used by analysts to get insights on connections and relationships within large datasets.
8. **Collaboration.** Information should be able to be organised in workspaces that can be shared within and between agencies and the private sector.
9. **Discover relationships.** A tool to visualise data that allows the user to experiment and apply 'what if' scenarios is needed.
10. **Alerting.** It's important that members of Australia's law enforcement AML community can create an ecosystem in which they are able to create a watchlist of objects, properties and relationships that proactively searches incoming data.

While these items represented the broad needs of investigative staff in operational agencies, their chief information officers (CIOs) were arguing for the development of solutions focused on fine-grained access control models, which promote access to data at the same time as enforcing access based on user credentials. This proposed identity management function for systems that rely on user identification for access is by no means inconsistent with the needs list proposed by operational participants.

Along a similar vein, financial industry participants discussed the need for improved secure communications with industry regulators and law enforcement agencies.

While private-sector vendor research participants were quick to highlight the value of cloud computing as an important technology in data access and sharing, many of the chief technology officers (CTOs) and CIOs or their representatives were less convinced. Australia's Digital Transformation Agency has followed the US Government's lead in making cloud-based platforms the priority for CIOs. The argument here is that it provides on-demand availability and scalability, increased network availability, increased engagement and interaction between users, rapid elasticity, futureproof technology and resource pooling.

We found that there was an indifference to cloud-based functionality among users and strategists. Causally, this may be able to be explained on the basis that users see no distinction between cloud and traditional provisions, and don't need to. In contrast, CIOs and CTOs have to run the systems that provide users with front-end functionality, which explains their reluctance to engage with such a blanket approach, due to the unique law enforcement and AML legislative impediments to data access and sharing.

AUSTRAC staff provided an interesting perspective that innovation in government tends to be dominated by discussions on technological capacity, such as cloud computing. Instead, AUSTRAC participants, as well as the private sector, posited that the real source of AML innovation stems from data itself as a key strategic resource. Key to this is the idea that the past 20 years of AML legacy has created a so-called 'system of systems' based on assumptions that now need to be retested before any decision on technological capacity is made. Ultimately, failure to address these assumptions led to bias being built into new systems and technological developments. This leads to a discussion on organisational culture and environments to promote innovative thinking and novel ways of engaging with data.

Cultures and organisational behaviours

An extensive body of literature highlights the link between organisational culture and innovation.[16] That literature also stresses that innovation is a relatively simple term to understand, yet the development of a culture of innovation eludes most organisations.[17] While the theatrical trappings of innovation, like beanbags and breakout rooms, might provide some framework for change, culture plays a far more important role. It's little surprise, then, that the research revealed a number of findings on the themes of culture and organisational behaviour.

During the research field phase, discussions of innovation in AML law enforcement often revolved around participants commenting on the impacts of specific technological products, financial accounting and the Department of Finance. Discourse analysis of these conversations could, on its own, lead to a hypothesis (*H1*) that the Department of Finance is inadvertently inhibiting innovation in exercising its established role as a 'gatekeeper'. But to do so would be incorrect, considering the context in which those observations were made. There can be little doubt that Finance uses controls over resources as a lever to instil economic and project delivery discipline across the public service as part of its role, but that need not be viewed as inhibiting innovation.

When analysed in more detail, the conversations on financial accounting and the role of the Department of Finance were more telling of the cultural and organisational construction of innovation and innovation management. Specifically, organisational cultural memory or perceptions of historical interactions with Finance and financial accounting systems was more likely to be inhibiting innovation. Often, interview participants would relay third-person stories of 5–10-year-old interactions with Treasury or Finance systems as evidence of the challenges they faced. A similar phenomenon was observed among vendors who highlighted how their relationship and commitment to working with agencies to develop technologically innovative responses were 'blocked' by Finance or Finance regulations.

However, the situation was often far more complex than these accounts, as formal decision delegations rest with agencies rather than the gatekeepers or policymakers. Similarly, it seems likely that local 'interpretations' of Finance policy may be what's restricting line agencies, when the intent of Finance may well be different from those local interpretations. Observations throughout the research phase revealed the need for improved communication and training on innovation processes and the role of Finance in those processes. One simple observation is that it's useful for line agencies to reach out to build working partnerships with Finance at multiple levels.

When these themes were explored further, the veracity of certain assumptions was found to be questionable. For example, despite its gatekeeper status, Finance looks to agencies for evidence that they're approaching innovation challenges with a clear problem definition, rather than demanding an exhaustive proposal for a platform or product solution. In this case, innovation could be further supported by staff education and training on problem definition in new policy proposals.

Overall, participants tended to indicate that public-sector organisational cultures may have conceptually conflated the innovation process (problem solving, future scanning and other similar processes or methodologies) with Finance's role and processes, when in fact line agencies have considerable autonomy in how they approach innovation and risk, but, as a legitimate part of government decision-making, must engage with Finance when seeking new funding. This hypothesis (*H2*) is further supported by the way that innovation success appears to be

measured in binary terms, insofar as an idea is considered successful if funding for it is received. Unfortunately, such a construction doesn't engage with the reality that most innovation ideas will end up being abandoned, and thus could disincentivise idea generation. In other words, some elements of observed cultural and organisational behaviour may be inhibiting the generation and consideration of new ideas.

Another interesting cultural observation goes to the nature of the innovation relationship between public-sector participants on the one hand and vendors and the private sector on the other. In many cases, we observed indicators of a combative relationship from some public-sector participants, who asserted the need for a strict compliance model for service delivery. When discussing the rationale for such 'hardline' approaches, public-sector participants provided historical case studies of past contractual failures by industry, often over many decades. In their recounts, participants articulated a rather stationary perspective on the private sector's ability to change and innovate. The finance-sector representatives went so far as saying that they felt law enforcement needed to be 'educated' on the banking sector. In doing so, while learning from the strengths of the financial sector is valuable, all parties also need to consider relevant findings from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry concerning gaps and shortcomings of the financial sector.

Accordingly, there's scope for improvement in public–private innovation and ICT relationships in the law enforcement sector, if not elsewhere. These observations reveal a need for investments in building a shared understanding of contractual relationships and expectations. There's meaningful scope here for the recently formed Home Affairs portfolio to explore new models for continuous and structured engagement with small, medium and large private-sector enterprises.

People

Much has been said about the changing nature of workplaces and workforces due to technological developments. Within the law enforcement landscape, many agencies are already trying to identify what skills and capabilities will be required by a police officer in 5–10 years. The AFP's *Policing for a safer Australia: strategy for future capability* report provides an example of this thinking.[18] The report also provides a glimpse of the future law enforcement workforce but stops well short of exploring its demands for new skills and the evolution of multidisciplinary investigative teams.

In the AML environment, people—or rather combinations of people with different skills and experience—are of critical importance to future success. Commentary on the demand for highly skilled workforces went beyond operational compliance or investigative staff in regulatory and enforcement agencies. However, while it's pertinent that the need for a future workforce is being discussed, participants were repeatedly unable to clearly articulate how those future requirements will be met.

Commentary often turned to discussions of the constraints of an arguably far-from-agile public service employment framework. Those conversations often reflected on how inflexibility on financial incentives for specialist staff and dated employment constructs—such as 'jobs for life'—prevented the kind of workplace renewal needed to address skills shortages. Much of this is inherited attitudes about previous rules and regulations. There's considerable flexibility in public-sector employment policies and regulations, although it might not be being used in as flexible and creative a way as is possible. This relates at least as much to organisational culture and the openness of leadership to taking advantage of flexibility as it does to constraints on public-sector employment practices.

We observed that discussions of people and innovation centred on three categories of staff: innovators, technologists and strategists.

Innovators are those staff formally—or often informally—responsible for developing and introducing new ideas, processes, methods and technologies. Participants revealed that informal or formal innovators in AML organisations were aware of the context of their individual roles and the business units they worked for. However, CIO and CTO staff often found that these innovators were less experienced or capable of situating their innovation work in the

broader organisational and whole-of-government contexts. Participants also regularly argued that their innovators were typically particularly skilled at one facet of innovation—technology, for example—but were less agile at navigating the various other technical aspects of innovation, such as finance.

In contrast to innovators, technologists are those who are capable of delivering innovation ideas through technology. Like the rest of the public service, the law enforcement and regulatory agencies charged with recruiting and retaining qualified and capable technologists face many challenges. Put simply, nearly every public-sector research participant stressed that technologist shortages impinged upon innovation.

One CIO argued that they had access to 'pockets of brilliance' but that most of their capability was in need of renewal. The argument was that these individuals have worked hard to keep innovation at a minimum level, often with 'sticky tape solutions'. Without whole-of-government integration, much of this innovation work is continuously at risk of perishing. Interestingly, micro-agencies such as AUSTRAC reported that they weren't experiencing such challenges.

It would be naive to argue that a solution for this issue can be found within the AML and law enforcement area. Rather, it needs to be resolved across the public service. At the very least, policymakers in the Home Affairs portfolio will need to consider the development of a human resources strategy to address these challenges. It seems almost certain that government will need to review some of the public service's employment arrangements to facilitate greater procurement of technologists.

That said, one area of comparative strength that was evident among the public service participants was the calibre of agencies' innovation strategists. Of particular note was the strength of the CIO and CTO cohort. There appeared to be genuine commitment among this group to the development of industry best practice in agile technological development and deployment. In many cases, there was also very high commercial acumen in managing vendors and users.

On broader skill sets, we observed that public-sector participants often applied a distinct agency-focused interpretation to AML policy and innovation. We considered that such approaches may inhibit whole-of-government innovation.

There was some discussion on the possibility of outsourcing or contracting innovation and technologists. Given the operating context presented by participants, it's likely that such an approach would end up as an unhelpful exercise of risk, shifting responsibility from strategic human resource management to contract management.

At the very least, we see an opportunity for Home Affairs to consider developing training and professional development options for its formal and informal innovators at the portfolio level. The focus of such efforts needs to be less on specific technological innovations and more on issues such as problem definition, whole-of-government integration, policymaking and finance.

Problems, not platforms

One recurrent theme in most of the interviews was the focus of technological innovation efforts. The discourse on this topic was highly diverse, but patterns began to emerge when the research sample was stratified by organisational role into vendors, operational agencies, central policy agencies and the finance sector.

Perhaps unsurprisingly, discussions about innovation with vendors[19] tended to gravitate to diagnoses of AML and law enforcement problems, complemented with a focus on solutions involving the use of their existing proprietary products. This was nearly always followed by grievances about the fixed nature of legislative and cultural impediments to technological innovation. However, it's important to note that vendor-generated innovation options didn't always engage with these policy challenges.

For example, legislative impediments to information sharing and data matching were the subjects of recurring anecdotes from vendors. Here, a vendor might seek to promote ideas on data matching across various departments. The proposal, while technologically sound and operationally beneficial, would never be realised due to legislative instruments such as the *Privacy Act 1998* (Cwlth) (information can be used only for the purpose for which it was obtained) and the AML/CTF Act (AUSTRAC data can be shared only with designated law enforcement agencies). Accordingly, there's an opportunity for government to work with the private sector to further enhance the sector's understanding of this legislation. For policymakers, this might also create the opportunity to establish a clearer model of what innovation is possible in technology and legislation.

Law enforcement culture is one of hard facts and the preparation of information for presentation in a justice system. Even at the national level, law enforcement is an operationally focused activity. It comes as little surprise, then, that the AML operational agencies' investigative and compliance staff often described their innovation challenges in terms of platforms or specific investigative impediments.

Investigative and compliance research participants reported that their understanding of technological innovation is often generated from personal contact with vendors. This was described as establishing 'what's out there' in terms of technology. And in this environment, AML technological innovation appeared to have a tactical aspect involving the preparation of *ad hoc* proposals and initiatives. Enterprise-level coordination of technology and innovation appears particularly complex and often combative in this environment.

In this tactically driven innovation space, we observed that CIOs and CTOs in operational agencies could be quickly preoccupied when faced with multiple time-sensitive incremental changes and their associated resource demands. The challenge here seems to be that this restricts the resources available to diagnose the specific problems that are being addressed. For agency CIOs and CTOs, this produces additional resource constraints on enterprise architecture and large ongoing costs for legacy and bespoke systems.

Interestingly, financial-sector participants had a much clearer problem-focused approach to AML. Their diagnosis of the problem relates to the need for enhanced real-time secure communications and the provision of threat and risk intelligence related to AML methodologies.

While this is symptomatic of the various drivers in play, there's a clear disconnect between the various stakeholders as to the focus of innovation. One way of addressing this issue may be to create innovation communities of practice within agencies or the Home Affairs portfolio. This isn't without precedent, as similar approaches have been used in at least one Australian intelligence agency. In such communities, the development of new technological innovation can involve drawing together innovators, technologists, strategists, policymakers and vendors much earlier in the innovation process. While some might argue that this approach might constrain thinking, the counter-argument is that it shares experience and broadens thinking and can also ensure that innovation ideas developed at the operational level will be underpinned by whole-of-agency and whole-of-government thinking.

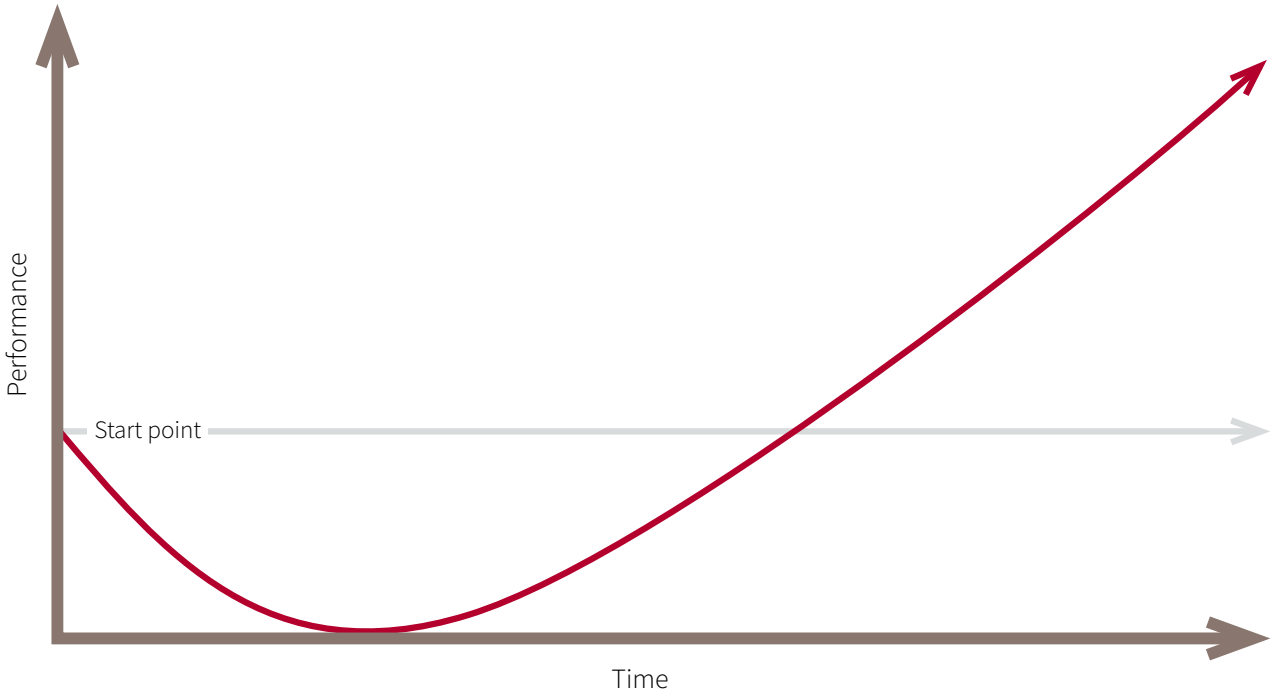
Budgets

It's a truism that the public sector never has enough resources to invest in all the worthy initiatives and innovations that it develops. Accordingly, while research participants voiced grievances about austerity measures, pertinent and policy-applicable themes about so-called budget hygiene factors also emerged.

There can be little doubt that historical approaches to technological innovation have left agencies with substantial budget legacy problems. Over the past couple of decades, Australia's law enforcement and Home Affairs agencies have initiated innovation projects that resulted in the development of various stand-alone data repositories and platforms. Those systems continue to have immense corporate and operational value. Unfortunately, their maintenance has large budget costs that are often, for the most part, unfunded as continuing line items. The continued investment in such systems draws important resources away from new innovation initiatives. In this space, the first question asked when new ideas are developed is 'What can we afford not to do?'

These observations give rise to another hypothesis (*H3*) about the funding of major innovation projects. Technological innovation and investments conform to the economic J-curve effect (Figure 2). In the early stages, project investments bring a negative organisational return. Over time, with changes in expenditure levels and project maturation, return on investment often exceeds the start point in successful projects.[20] The implications of this economic projection for the public sector are twofold. First, monetising benefits of major projects in an accurate and meaningful manner is difficult, as return flows are hard to predict, particularly where they're in the form of avoided costs or non-monetary benefits such as arrests or disruptions. Second, contract and budget lifecycles prevent the development of consistent road maps for innovation when uncertainties persist. Hence we often see today's technological initiative become an unfunded legacy system, the maintenance of which is made challenging by Finance's rules on operational and capital expenditure.

Figure 2: The J-curve



The establishment of the Home Affairs portfolio offers a rare opportunity for the government to determine a baseline for the legacy costs of its systems. Through economies of scale in portfolio budgets, there's greater opportunity for longer term budget certainty and, in turn, forward planning for system maintenance.

Cooperation and collaboration

Public–private collaboration on AML is a given. The level of ongoing engagement is evolving and increasing, and is met with a genuine desire for public–private partnerships. However, despite widespread success, there remain areas ripe for further improvement.

Throughout the research, vendors and finance-sector participants highlighted what they considered to be ongoing disconnects between programs and outcomes. In the case of the finance sector, many comments were made about how further cooperation and collaboration in AML intelligence and communication would contribute more to outcomes than would developing specific in-house programs. In particular, there's a clear need for greater feedback between regulatory and enforcement agencies and the private sector on the utility of finance-sector information.

Another recurrent theme throughout the research interviews was the critical—albeit unrealised—role that mid-level agency officials (Executive Level 1 and 2) play in interagency cooperation and cross-sector collaboration.

As a unique case study, Finance participants related that structured engagement between Finance and the Department of Defence through the Defence Strategic Investment Committee at the deputy secretary level had markedly improved the take-up of innovation. Early project engagement across agencies resulted in demonstrable improvements in the quality of submissions to Finance and passage through project gateways. While Defence projects differ markedly from projects in Home Affairs in their quanta of financial investments and lifecycles, this observation does support the merits of closer interagency cooperation and cross-sector collaboration on AML innovation.

Agility

Agility in innovation is a subjective, aspirational term, rather than denoting a specific achievement. There should be little doubt that there's substantial evidence that the public sector, and more specifically federal law enforcement, has made significant progress in innovation and project agility. Similarly, consecutive government efforts to reduce bureaucracy have made important advances. However, public-sector participants consistently highlighted that more can be done, for which they eagerly offered detailed recommendations.

Nearly all participants lamented that policy proposals and new policy initiatives remain underpinned by a focus on accountabilities measured by 'doing things right' and 'doing things as planned'. While that may well reduce implementation risk, it can also reduce incentives to pursue opportunities while taking risk. A too dogmatic pursuit of proper process could be viewed as a disincentive for 'doing the right things'. The rapidly evolving law enforcement and technological operating environment means that defining the innovation problem in exact terms at initiation is increasingly difficult, if not impossible, and perhaps even misguided. Further, the lifecycles of projects and project outputs are becoming dramatically shorter. For example, the AFP's current case management system is some 30 years old, but its replacement is likely to be operating for only a fraction of that period.

In this environment, traditional command structure models were considered to be inhibiting innovation and change. A number of the CIOs interviewed were responding to the changing environment by flattening organisational structures and embedding technologists in innovation initiatives. Those efforts, however, continue to be hindered by government's conventional contractor models, in which contacted technologists have limited decision-making powers and are engaged on short-term contracts (of one year or less), preventing sustained investment in complex issues.

Risk

Several risk issues were raised during the field phase of the research. Many participants recognised that the rapid evolution of technology is increasing the risks in technological innovation projects, even for short-term and piecemeal endeavours. Perhaps this viewpoint is itself symptomatic of a misunderstanding about the nature of new technology developments. The opposing argument to those perspectives is that being able to progress from developmental idea to operating solution faster by using new approaches to building applications results in less risk of failure than that found in large, lengthy ICT systems development projects.

The private-sector vendors argued that federal agencies need to assess risk differently. One vendor explained:

> While we are an area that requires extreme diligence, we understand that in practice achieving 100% doesn't work anymore and the last 20% is often impossible to achieve and has diminishing levels of return on investment.

Operational agencies were particularly critical of the procurement governance arrangements and perceived that they contributed to unhealthy levels of corporate fear of failure. According to practitioners, processes—rather than outcomes—had become a corporate priority, which contributes to unhealthy levels of corporate fear of failure and ultimately inhibits innovative risk-taking.

A Department of Finance representative vehemently opposed those perspectives. Drawing upon the previously explained case study of the Defence Strategic Investment Committee, the representative drew attention to the uneven maturity in enterprise investment committees across government. It's important to note that the representative also hastened to advise that law enforcement acquisitions tended to demand less long-term planning and smaller budgets than large defence projects. However, the bottom line is that strategic investments in Australian AML enforcement are overwhelmingly focused on operational tools and are rarely examined through a holistic long-term lens like that used for defence capability investments.

Decision-making

Strategic foresight in the AML environment is limited by the extent to which analytical models can anticipate how future information flows and scenarios will evolve. The ability to apply forward thinking to adapt to the evolution of organised crime fundamentally requires innovation. On this subject, Max Bazerman argues that 'Finding the best solutions often requires dropping the proposed options and looking beyond the immediately obvious.'[21]

However, various research participants contended that bureaucratic overheads for innovation were too high to facilitate Bazerman's call for curiosity. In particular, decision-making on technological innovation in the public sector too often defaults to a short-term focus. That focus was attributed to the low appetite for risk and high demand for immediate returns on investment—the so-called 'tyranny of the tangible'. Admittedly, as the turnaround times for ICT shorten, the concept of long-term investments may need to be reconsidered.

Vendors noted that long-term decision-making can be facilitated by clearly articulating problem definitions and setting the parameters of flexibility early. This way, vendors can be encouraged to be meaningfully involved throughout the innovation cycle.

IMPLICATIONS

Clearly, this body of research has a number of implications for policymakers seeking to drive technological innovation in Australian AML enforcement and compliance. When it comes to specific innovative technologies, there have been significant advances in big-data technologies over the past few years. Such advances offer new capabilities that may enhance the collection, collation and analysis of information. Nevertheless, private- and public-sector enthusiasm in this space needs to be tempered by a greater understanding of legislative and ethical barriers as well as technological and methodological limitations.

Innovators and strategists alike need to carefully ensure that government understands that predictive analytics aren't a panacea for random events or the unknowable future. Predictive analytics extrapolate functions of best fit based on past data to determine what the future is most likely to look like. Accordingly, it's unlikely that those processes will foresee inflection points beyond the data used to construct the model. This, of course, is the place for the innovators.

It seems almost certain that future technological innovation will largely be done by industry, not government. The days of DARPA-like[22] agencies developing technologies that eventually become commercial opportunities are no longer the norm. The private sector's perspectives converge around the acknowledgment that this reality is having lasting impacts on public-sector technological innovation. Most solutions will now be commercial-off-the-shelf, which meets 80% of government requirements. The final 20% of functionality will be developed through government working with an ecosystem partner. While many public-sector officials might not agree with that model, or feel that having such close strategic partnerships with the private sector is problematic, it seems the most viable model available.

Law enforcement innovation agendas, especially for AML, face a number of organisational and cultural challenges. In many cases, we observed three broad issues: innovation cultures, innovation focus, and innovation integration.

The evidence seems clear that communities and nations will experience increasingly more frequent technological disruptions that will revolutionise our way of life. Those disruptions will appear outside of conventional thinking, but will rapidly be accepted and normalised. Engaging with such new thinking, new opportunities, new risks and new threats requires cultures of innovation in enforcement and regulatory agencies. In this environment, government will need to avoid being preoccupied with the trappings and theatre of innovation and instead prove disciplined in its pursuit.

As Heda Segvic says, 'No one errs willingly.'[23] Innovation is a particularly precarious space, where 'faults are inevitable, [and] important events, disruptive innovations, and "black swans" constantly test the experts' professionalism and crisis management skills'. This research provides sufficient evidence to support the idea that the federal law enforcement community, and the wider public service, is adept at responding to such challenges. However, we found less evidence that organisational frameworks for enterprise or portfolio technological innovation are fully developed. Despite the existence of various pockets of innovation excellence in Australia's law enforcement community, there are indicators of cognitive bias in some of the thinking about technological innovation, and about what the rules that they feel bound by are—whether on procurement or employment. In

many cases, there was a symmetry in agency responses that could also be evidence of the need for more contested policy perspectives and advice and a clear need to engage more with central agencies to move beyond perceptions and towards working partnerships.

Overall, this research revealed that the focus of technological innovation in AML is often preoccupied with specific platforms, tools and capabilities at the expense of more strategic thinking. There didn't appear to be any long-term strategic road map guiding innovation in federal law enforcement, and what little was present was broad in guidance and unfunded.

Strategic investments in this space are consequently focused on operational tools and are rarely examined using a holistic long-term lens like that used for defence capability investments. Outside of the scope of AML, the newly formed Home Affairs Department continues the work of its predecessor, the Department of Immigration and Border Protection, in addressing this issue. While potential advances are difficult to quantify, the literature suggests that this approach might not result in the realisation of medium- and long-term benefits. Such approaches may also have short- and long-term innovation opportunity costs. As discussed, the ongoing cost of maintaining access to outdated, stand-alone legacy systems in Home Affairs and the AFP is a particularly problematic example.

In practice, the benefits of technological innovation may be limited at the idea-generation stage due to an overconfidence in operational staff's capacity to diagnose innovation problems and their impacts on the enterprise. The traditionally closed nature of the law enforcement community and its bias towards its own can often prevent the penetration of new thinking. The impacts of that bias appear to be reinforced by an accountability system focused more on the bureaucratic structures of project management and financial accountability than on innovation and outcomes.

Taken together, these observations support a further hypothesis (*H4*): that innovation in AML is habitually more akin to a cottage industry. Long-term architectures and strategies for technology innovation integration aren't being widely considered beyond the CTO and CIO cadre. Therefore, technologies aren't well integrated across organisational strategies, across portfolios, or across the whole of government.

However, by no means does this report argue that technological innovation isn't occurring, or that agencies don't have the right people. Rather, the law enforcement sector is ready with time and capability for a disruptive change of its own. The key to that disruption won't be innovation theatre or trappings, but a far more tangible change and commitment.

POLICY RECOMMENDATIONS

In response to this body of research and its implications, we make the following recommendations.

Recommendation 1. In response to the challenge of innovation, Home Affairs examines how innovation culture broadly, and technological innovation more specifically, can be further nourished in its portfolio agencies.

Recommendation 2. Home Affairs explores how the centralisation of technology budgets and innovation management in the Home Affairs portfolio might resolve issues such as cognitive bias, innovation economies of scale, and interagency innovation integration.

Recommendation 3. Home Affairs develops an innovation strategy in consultation with its portfolio agencies. That strategy ought to provide a clear and shared definition of innovation, outline roles and responsibilities, and formulate comprehensive innovation metrics.

Recommendation 4. All agencies identify mechanisms relevant to their organisational structures for earlier engagement with the Department of Finance, perhaps learning from the engagement between Defence, Finance and the Department of the Prime Minister and Cabinet on defence investment.

Recommendation 5. Across the federal law enforcement community, agencies nominate accountable and capable innovation leaders to promote and support innovation.

Recommendation 6. All agencies continue to emphasise the importance of problem definition to innovation. In doing so, agencies ought to promote greater engagement with non-technical solutions to innovation, including facilitating a shift from rules-based to agile risk-based responses.

Recommendation 7. Home Affairs establishes new panel mechanisms for engagement with industry and academia to regularly discuss emerging disruptive ideas and technologies. This needs to be viewed as an ongoing activity involving representatives from across the Home Affairs portfolio agencies. This should be augmented with mechanisms to engage with individuals and start-ups working at the emerging edge of new thinking. Measures such as competitions focused on solving specific innovation or technological challenges could also be used.

Recommendation 8. All agencies emphasise working more collaboratively with the finance sector through such measures as:

- AUSTRAC establishing a regulatory sandbox to explore new policies and offsets for those companies that can contribute to AML efforts
- ACIC establishing a capability with responsibility for sharing AML intelligence with the Australian financial sector.

Recommendation 9. Corporate innovation management needs to be further standardised across Home Affairs portfolio agencies.

CONCLUSION

Innovation requires an ability to monitor what's happening in change and technology. Then an agency must be able to find the time, space and resources to consider the problem and alternatives. Throughout this process, the work of innovation must prioritise the role of the wider agency, portfolio and whole-of-government innovation focus and policies: tough choices about prioritisation are a given in law enforcement. Further, each of the stakeholders must be agile enough to change and adopt those innovations that could be conceived as 'quick wins'. It's certainly no easy task.

This paper has focused on one particular crime type—money laundering—and on one layer of government—the federal level. Increasingly, technological developments and the globalised world ensure that crimes are becoming cross-jurisdictional or even multijurisdictional. Accordingly, technological innovation at all levels is becoming ever more critical. Innovation will be needed to move traditional law enforcement modalities of occasional links to increasingly standardised connections.

As a starting point, collective awareness of future challenges could be the catalyst for shared innovation opportunities. Co-design and cooperation on the development of innovative law enforcement approaches offers a plurality of cross- and multijurisdictional benefits. Australia is well positioned to play an active bridging role to help other jurisdictions to better anticipate, understand and respond effectively to ever-evolving organised crime.

NOTES

1 John Coyne, 'Encryption: the perils of "going dark"', *The Strategist*, 22 August 2017, online.
2 In this report, 'innovation' is used to refer to the process by which new and better solutions are developed to meet requirements, unarticulated needs or existing needs.
3 Parliamentary Joint Committee on Law Enforcement, Inquiry into the impact of new and emerging information and communications technology, online.
4 AUSTRAC, *FTR Act: about the FTR Act*, 11 December 2014, online.
5 Financial Action Task Force (FATF), *Third mutual evaluation report on anti-money laundering and combating the financing of terrorism: Australia*, FATF, Paris, 14 October 2005, online.
6 AUSTRAC, *FTR Act: about the FTR Act*
7 Attorney-General's Department (AGD), *Report on the statutory review of the Anti-Money Laundering and Counter-terrorism Financing Act 2006 and associated rules and regulations*, Australian Government, 2016, online.
8 AGD, *Report on the statutory review of the Anti-Money Laundering and Counter-terrorism Financing Act 2006 and associated rules and regulations*, 45.
9 AGD, *Submission of the Attorney-General's Department Senate Economics References Committee Inquiry into digital currencies*, AGD, Canberra, 2014, online.
10 This amendment is the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cwlth).
11 AUSTRAC, *Chapter 6: AML/CTF programs*, 29 July 2016, online.
12 Michael Doran, Michael Janda, 'Commonwealth Bank to pay $700m fine for anti-money laundering, terror financing law breaches', *ABC News*, 4 June 2018, online.
13 FATF, APG, *Anti-money laundering and counter-terrorist financing measures: Australia: mutual evaluation report*, April 2015, online.
14 FATF, APG, *Anti-money laundering and counter-terrorist financing measures: Australia: mutual evaluation report*, 7.
15 The commentary in each point is a summation of the information provided by research participants and doesn't necessarily reflect the authors' perspective.
16 NN Taleb, *The black swan: the impact of the highly improbable*, Random House, New York, 2007.
17 Department of Industry, Innovation and Science, *Innovation*, Australian Government, 20 November 2017, online.
18 Australian Federal Police, *Policing for a safer Australia: strategy for future capability*, Australian Government, March 2017, online.
19 It's important to note that the vendor sample comprised representatives from large ICT providers, so the validity of observations should be viewed through that lens.
20 Noting that many innovation efforts fail.
21 M Bazerman, *The power of noticing: what the best leaders see*, Simon & Schuster, New York, 2014.
22 DARPA: Defense Advanced Research Projects Agency (US).
23 H Segvic, 'No one errs willingly: the meaning of Socratic intellectualism', *Oxford Studies in Ancient Philosophy* (ed. D Sedley), vol. XIX (Winter 2000), Oxford University Press, Oxford, 1–45, online.

ACRONYMS AND ABBREVIATIONS

ABF	Australian Border Force
ACIC	Australian Criminal Intelligence Commission
AFP	Australian Federal Police
AML	anti-money laundering
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cwlth)
AUSTRAC	Australian Transaction Reports and Analysis Centre
CIO	chief information officer
CTF	counter-terrorism financing
CTO	chief technology officer
FATF	Financial Action Task Force
ICT	information and communications technology
R&D	research and development

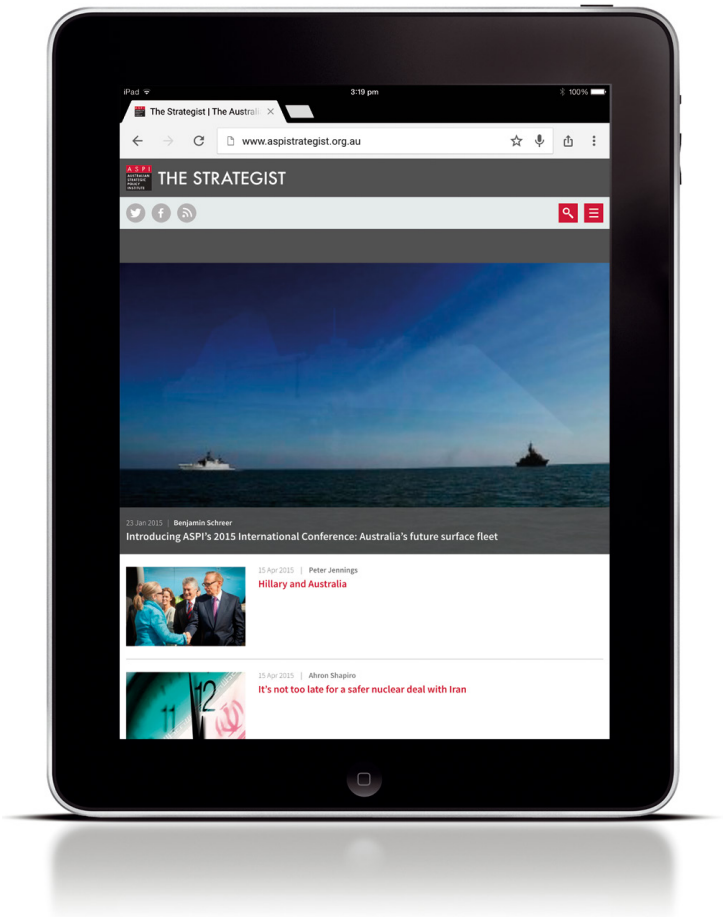
WHAT'S YOUR STRATEGY?

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.

facebook.com/ASPI.org

@ASPI_org



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Supported by

LOCKHEED MARTIN · NAVAL GROUP · Raytheon Australia · KPMG

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.

I can see clearly now!
Technological innovation in Australian law enforcement:
A case study of anti-money laundering

ISSN 2200-6648