STRATEGIC INSIGHTS

ASPI

Towards a Commonwealth law enforcement innovation framework

147

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Genevieve Feely and John Coyne

Introduction

In March 2019, ASPI, with the sponsorship of Oracle, coordinated the ASPI–Oracle Innovation Framework Workshop. The workshop brought together subject-matter experts from federal law enforcement agencies, academia and the private sector to explore the feasibility of a Commonwealth law enforcement innovation framework (CLEIF).

This followed a 2018 research project that explored the current state of innovation in law enforcement.[1] That research was based on a case study of innovation in Australia's federal anti-money-laundering (AML) provisions. The 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?

Vintage police sign and light: iStockphoto/moisseyev.

August 2019

The research resulted in the publication of a Special Report, titled 'I can see clearly now!', which provided specific analysis of the key factors that support and restrict technological innovation in federal law enforcement AML efforts.[2]

The report's central argument was 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.

While the research was focused on technology and AML, it has broader application to law enforcement technological innovation. The research found little evidence that the organisational frameworks for enterprise or portfolio technological innovation in federal law enforcement are fully developed.[3]

The March 2019 workshop explored innovation themes in government and the corporate sector that had relevance to law enforcement. The results provide further input to policymakers as they formulate future directions for the agencies and their capabilities.

Purpose

This report presents the key innovation themes that were discussed during the workshop before presenting a SWOT analysis for the implementation of a CLEIF.[4] The aim is to promote further consideration of the concept of such a framework.

Methodology

The workshop was conducted on 12 March 2019 under the Chatham House Rule. The agenda was divided into five sessions:

- The context
- Innovation in law enforcement: a case study of the Fintel Alliance
- Innovation in research: a case study of the Data to Decisions Cooperative Research Centre
- Innovation in the private sector: a case study of Oracle
- A SWOT analysis of the concept of a CLEIF.

The context

In this space, 'innovation' refers to industrialising the generation of new approaches. For many years, governments haven't had a significant independent technological edge except in niche areas. Much of their advantage has been created by companies in sectors that are dependent on government spending—notably defence, with some contribution from in-house government R&D through entities such as Defence Science and Technology and its predecessor groups. This situation has shifted over time, and the dominant source of innovation is now commercial sectors that aren't primarily driven by government investment and aren't primarily in the defence sector. The result is that, in the face of rapid technological change, governments need to find new ways of accessing a technological edge. The very concepts of sovereignty and geographical jurisdictions are being challenged, given the globalised nature of some technologies, corporations and activities (finance being an obvious one of relevance to law enforcement).

At the turn of the millennium, cutting-edge computing capability was still being driven by governments, or at least by government demand. However, the speed at which technology has been developed and then deployed has since accelerated exponentially. In the process, the Australian Government's technological advantages have eroded. 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, and not just in Australia.

More recently, technological developments, especially those that have been disruptive, have subsequently been driven predominantly by private corporations.[5] Legislative responses to those changes, disruptive or otherwise, have lagged the changes. In some cases, the corporations responsible for the changes draw their 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. 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.

By the early 2000s, our day-to-day life was mostly viewed by policymakers through two conceptual lenses: real and virtual, with quite a clear separation between the two realms. Governments' 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 the 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.[6] ASIO Director-General Duncan Lewis has recently argued that 'a person who would wish us ill is far more empowered as a result of the technology at their disposal than once upon a time.'[7] State and non-state actors alike are leveraging technology to communicate, mount 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 limitations on the capacity of law enforcement here and elsewhere 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 because they operate in ways that aren't vulnerable to existing police capabilities and legislative powers. The range of transnational untouchables—those that 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, differing rules across jurisdictions and the effectiveness of cross-border cooperation. While criminal organisations can cross borders in seconds electronically, the collection of evidence from individual foreign jurisdictions 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), with intelligence from Israel, uncovered a suspected Islamic State plot to blow up an Etihad flight to Abu Dhabi. The terror group allegedly coordinated the operation in Syria and mailed a bomb kit from Turkey.[8]

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. Clearly, this requires new skills in law enforcement entities as well as new concepts for applying these new analytic tools.

The impact of new and emerging information and communications technology (ICT) ensures that technological disruptions will increase rapidly—and the resulting need to adapt should be built into agency business models. The implications of the current trajectory of technological developments is that the life cycle 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.

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

Law enforcement has traditionally employed a 'grow your own' approach to subject-matter expertise and capability development. In the current operating context, it will also need to engage more frequently to acquire capabilities and subject-matter expertise on an as-required, contracted basis, putting expertise into the investigations at hand when needed. R&D budgets for law enforcement, especially for the development and rapid fielding of technological capabilities, need to drastically increase. Martin Callinan makes this point in his 2019 ASPI Special Report, *Defence and security R&D: a sovereign strategic advantage*.[9] 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, financial and policy dimensions.

Key points

1. Innovation is increasingly coming from commercial sectors that aren't primarily driven by government.
2. The Australian Government's ability to be a dominant driver of technological innovation has ended.
3. Opportunities to adopt commercial innovation are strong, and the government's ability to seed innovation from R&D funding can push innovation into paths useful to law enforcement.
4. Innovation isn't just about available finance but about entrepreneurial approaches to technological innovation.
5. Technological disruptions to the way our world operates are becoming more frequent and potent—and perhaps need to be thought of less as disruptions than as rapidly emerging opportunities to change the way agencies operate.
6. 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.
7. R&D budgets for law enforcement, especially for the development and rapid fielding of technological capabilities, need to drastically increase and be used to drive private innovation that law enforcement can use.

A law enforcement case study: the Fintel Alliance

Launched in 2017 by the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Fintel Alliance is a private–public partnership established to combat money-laundering and terrorism financing. The alliance is between the federal government and the finance sector.

It's structured with two hubs: an Innovation Hub and an Operations Hub. Individuals from various private-sector finance organisations are seconded into the Fintel Alliance, which allows for higher levels of collaboration.

The Innovation Hub activities are either 'push projects' (that is, looking at ways new technologies may be employed in an operational scenario) or generated by the Operations Hub identifying operational problems to be solved with technology. The Innovation Hub develops capability, through proof-of-concept with the Fintel Alliance members, which is then moved across to the Operations Hub.

Two recent examples are the Pseudocode and the Alerting Platform projects.

- Pseudocode allows the Fintel Alliance to identify criminal networks using data drawn from all stakeholders, and to develop typologies in order to improve reporting of suspicious individuals and behaviour.
- The Alerting Platform Project is a longer term one and is a form of confidential computing whereby users can use data without seeing information. This approach to anonymising data but still enabling it to be useful in data analysis is a promising design approach to address privacy concerns and legislative restraints on the use of personal information.

This division of innovation and implementation could be a useful adaptation for the CLEIF, as innovation could occur centrally in conjunction with various stakeholders and be operationalised in various operations hubs as needed by agencies.

Key points

1. Innovation projects with multiple stakeholders that cross sectors are complex. Participation isn't mandatory, and contributions can vary. An innovation framework needs to consider that an equal contribution from each stakeholder may be unlikely—and stakeholders must be comfortable with this as a design principle of the partnership.
2. Centrally managed innovation frameworks need to proactively engage with those responsible for operationalising projects throughout the innovation process.

Innovation in research: the Data to Decisions Cooperative Research Centre

Cooperative research centres (CRCs) were pioneered by the Australian Government during the 1990s to support collaboration among government, industry and researchers and foster high-quality research and outcomes. Since then, the government has committed nearly $5 billion in grants to CRC projects.

The Data to Decisions (D2D) CRC is a collaboration between national security agencies, industry and researchers.[10] The D2D CRC was established as a five-year project with the purpose of solving big data challenges facing the Australian national security community. It currently runs four R&D projects, which all focus on harnessing the power of big data to create predictive and analytical functions for national security and law enforcement agencies.

After five years, this particular CRC is nearing the end of its life cycle; however, it has spurred the creation of two new start-ups (Fivecast and NQRY) to continue the innovation generated in the research projects, showing the potential for work from CRCs to become self-sustaining and attract funding from other sources as well.

The D2D CRC provided several key insights on its innovation journey. The first is the need to remove the fear of failure ('fail fast' is an easy motto but a much harder thing to demonstrate in practice). During its first years of operation, D2D was frequently faced with decisions that involved significant implementation risks. There was a need to balance necessary risks in innovation against insulation from failure. In doing so, D2D made failure not a thing to be punished or frowned upon but an inflection point for learning.

The second key insight was the need for innovation champions who not only support but understand the innovation process.

The real benefit of a CRC is its ability to draw together a variety of stakeholders and bridge the public–private divide.

Workshop discussions following the presentation of the case study highlighted the inherent challenges of traditional law enforcement performance indicators for technology development. A key observation is that often law performance measures for enforcement technology projects are more centrally focused on time and budget delivery, which makes the application of more agile R&D approaches challenging.

The D2D CRC case study highlighted that there are often numerous opportunities for policymakers to propose changes to legislation and policy constraints that are currently unintentionally inhibiting innovation. Such changes require organisations to adopt a more entrepreneurial mindset that looks to digital transformation and innovation to keep pace with increasingly frequent technological disruption. While legislative change isn't easy, it was recognised that many legislators are looking to boost industry and bridge the public–private divide.

Key points

1. Fear of failure restricts innovation.
2. Project failure is inevitable in innovation, and organisations need to be able to stop projects when it becomes obvious that success is unlikely.
3. Innovation projects need strong champions.

Innovation in the private sector: a case study of Oracle

Oracle provides essential services and products for companies to pioneer innovations and drive new business models. For example, Oracle embeds machine learning into several management and security offerings to help monitor, troubleshoot and predict potential outages and security breaches. Its corporate focus is on integrating artificial intelligence into analytics to help discover hidden patterns and enable automated and personalised interactions across applications via digital assistants. Oracle helps customers develop road maps, migrate to the cloud and take advantage of emerging technologies from any point: new cloud deployments, on-premises environments, and hybrid implementations.

As a large multinational organisation working across industries in both the private and public sectors, Oracle provided the workshop with a series of insights into how to develop and promote an innovation culture.

Oracle's innovation framework centralises 'innovation management' to be able to identify sources of innovation and then direct resources towards economically profitable innovation.[11] It uses a five-step structured process, known as the Oracle Innovation Design Engine, that supports end-to-end innovation: frame, ideate, share, test and scale. This can also be conceptualised as building an 'innovation pipeline'.[12] Using this structured process, the best ideas can be chosen and finessed.

Discussions on profit suggested that the private sector's profit motive could be replaced with a balanced return on investment consideration, in which a reasonable profit return sits alongside a longer term revenue flow.

Importantly, Oracle emphasises benefits from continual, at times incremental, innovation and moving away from the idea that adding or creating value can only come from radical change and innovation—an idea that should be emphasised in creating a CLEIF.

Additionally, Oracle seeks to inculcate and nurture a culture of innovation. Principally, the argument is that culture is the key catalyst for innovation. However, to be successfully developed the innovation must be championed at a high level within the organisation.

Oracle argues that organisations can't adopt a business-as-usual approach to innovation, which is why leadership engagement is essential. To be successful in the private sector, innovation and the processes for managing it must be continuously adapting.

Key points

1. Culture is a critical input to innovation.[13]
2. An innovation framework should be viewed as a prioritisation tool that promotes the creation of an endless line of potential opportunities and possibilities; however, inevitably, most will never reach full implementation.
3. The decision-making in a public-sector innovation framework would need to be driven by a balanced scorecard return-on-investment calculation that also considers the opportunity costs of not adopting specific innovations.
4. Innovation needs to be viewed through two lenses: radical change and incremental change.

Constructing a law enforcement innovation framework

Each of the case study sessions resulted in substantial discussion among the participants. That conversation, while broad ranging, revealed that more can be done to enhance innovation in federal law enforcement. More specifically, the workshop's first four sessions revealed that a CLEIF was likely to be needed and demanded.

The final session was used to undertake a SWOT analysis of such a framework.

Strengths

During the workshop, strengths were conceptualised as characteristics that could give a CLEIF an advantage over other approaches to innovation. The following specific strengths were identified during the workshop:

- There are already good examples of collaboration underway, such as the Fintel Alliance and the D2D CRC. It's easier to conceptualise and construct a framework when good examples are already thriving.
- There's also much goodwill, intent and interest in continuing these existing arrangements, which could lead to interest in establishing new ones.

Weaknesses

Weaknesses were conceptualised as characteristics of a CLEIF that may place it at a disadvantage compared to other systems. The following specific weaknesses were identified during the workshop:

- One of the principal weaknesses is the public sector's fear of failure and its risk-averse attitude. That attitude has a very legitimate basis: the misallocation of taxpayers' funds is rightly a significant concern for all public-sector agencies and entities, and failure on innovation can often be characterised as waste. However, as much as possible, that attitude should be minimised, including by being able to derive benefits and lessons from 'failed' innovation. Organisations need to nurture innovation cultures and promote engagement with risk.
- A CLEIF could place too much emphasis on creating new products constantly instead of reusing, recycling and adapting existing and appropriate technology. It would need to give some focus to regular stocktakes or near-real-time management of current technology and projects.
- Centralised objectives and resourcing make it difficult to enunciate and change priorities and objectives as quickly as needed. Agility and the ability to adapt quickly are necessary for innovation to thrive, so this will have to be addressed in any CLEIF model proposed.

- There have been some concerns that not enough future policymakers from younger generations are involved in the innovation and project process, and that they should be better nurtured and given senior leadership support as they engage with risk.

Opportunities to be seized

The workshop identified the following opportunities:

- New and innovative partnerships are starting in a whole range of areas. Consideration could be given to how those relationships could be further leveraged from a federal law enforcement community or whole-of-government perspective.
- There are numerous opportunities to propose changes to legislation and policy constraints. Doing so in the context of innovation may perhaps be particularly attractive to legislators who are looking to boost industry and bridge the public–private divide.
- There's an opportunity to explore new and meaningful key performance indicators to give a more realistic assessment of how law enforcement technology is progressing.

Threats to be controlled

Several threats need to be considered while planning a CLEIF:

- In technology, crime is outpacing law enforcement every day of the week, mainly because it's opportunistically hitchhiking on wider commercial innovation and technology.
- The pace of innovation in the broader community continues to increase. In response, law enforcement will have to constantly scan the horizon to anticipate changes, and it needs partners immersed in commercial innovation to add their own scanning capacity.
- Organisational structures can be a threat to the implementation of innovative practices. For example, at the state and federal levels, law enforcement agencies have different, and sometimes competing, priorities. The jostling for resources and attention could be managed in an integrated system to ensure the most effective use of time and resources. Related to this will be how priorities are set so all stakeholders see that they're getting the maximum value-add for their contribution.
- During decision-making, there may be conflicting objectives between decision-making and what will address the issue. This will have to be mitigated by open analysis and frank conversations about issues and priorities.
- Public engagement about the reasons for shifts in concepts of operation and technology and, where relevant, legislative change to enable those shifts will require well-designed public engagement and communication if community support is to be achieved.
- As financing is a clearly identified issue, all key law enforcement agencies and departments need to find a dedicated budget line or other sources of funding for innovation, which might be best channelled through a centralised hub to achieve critical mass and efficiency. This should be an attractive prospect for central government agencies involved in financing as it will streamline the cost of innovation into a single location.

The framework

To be successful, an optimised CLEIF would:

- integrate all levels of law enforcement and national security activities
- have reliable and flexible funding
- take into consideration the wide range of stakeholders and their needs
- widen the sources of innovation and innovation scanning beyond law enforcement agencies to include capable commercial partners.

An entity structured similarly to the CRC model would offer flexibility and opportunity to create innovative solutions for law enforcement. However, while having a model that sits outside of government has advantages, there are legislative barriers that would need to be considered. For example, certain provisions of the *Privacy Act 1988* (Cwlth) will make it extremely difficult to share the necessary information from law enforcement and national security agencies with a CRC, hindering its capacity to properly address problems and create solutions.

In all likelihood, a well-designed CLEIF will have to integrate a number of different approaches in order to ensure that the agencies involved continue to meet their legislative obligations.

Considering all of the issues discussed in this workshop, consideration could be given to the next steps:

- the signing of a memorandum of understanding (MoU), initially by all relevant federal agencies, to inculcate a culture of innovation in this space
- the creation of a law enforcement innovation hub in the Australian Criminal Intelligence Commission.

Memorandum of understanding

The MoU would articulate a principles-based commitment by federal law enforcement agencies to work together on innovation. However, this early federal focus should be a starting point only; the end goal would be the inclusion of state and territory agencies.

The MoU could be focused, at least initially, on four key priority areas:

- developing and documenting the agencies' innovation cultures
- documenting and sharing innovation projects
- working within legislative and regulatory requirements, a commitment from each agency to resource innovation projects
- a commitment to burden share law enforcement community challenges.

Law enforcement innovation hub

At this initial stage, a collaboration research hub could provide a starting point for creating and developing new technologies for law enforcement. While some stakeholders may be tempted to adopt a CRC-type structure, a stronger starting point might involve building on initial interest in cooperative innovation among law enforcement stakeholders.

A committee supported by a modest secretariat in either the Australian Criminal Intelligence Commission or the Department of Home Affairs could be used to promote exchanges of knowledge on innovation. It could focus on sharing current and future innovation investments and challenges. The secretariat could be used to develop central innovation challenges and projects registers with the aim of identifying opportunities for burden sharing and collaboration.

Conclusion

Partnerships and co-creation are crucial to the future successes of Australia's law enforcement agencies. The workshop, supported by ASPI's earlier report, made a solid case for a cohesive and coherent CLEIF to encourage change in law enforcement's innovation culture and behaviours. A focus should be on preventing innovation silos. While the workshop identified a need for change, and this report has provided some initial steps, further research and collaboration are needed before a definitive framework can be developed.

Before engaging in a program of change, it's imperative to acknowledge that a great deal of innovation, both technology-based and not, already occurs within and across the various stakeholders who attended the workshop. That work has also had very real positive impacts on community safety. Similarly, the commitment of those from the public, private or not-for-profit sectors who attended the workshop, as well as those who participated in the preceding research projects, speaks volumes of their contribution to collaboration and innovation. The central thesis here isn't a critique of what's being done, but rather a strong argument for how to leverage current efforts to achieve even more.

Notes

[1] John Coyne, Amelia Meurant-Tompkinson, 'I can see clearly now! Tech innovation in law enforcement', *The Strategist*, 19 July 2018, online.

[2] Coyne & Meurant-Tompkinson, 'I can see clearly now!'.

[3] Coyne & Meurant-Tompkinson, 'I can see clearly now!'.

[4] SWOT = strengths, weaknesses, opportunities and threats.

[5] Coyne & Meurant-Tompkinson, 'I can see clearly now!'.

[6] Coyne & Meurant-Tompkinson, 'I can see clearly now!'.

[7] Colin Brinsden, 'Australia faces daily threats: spy chief', *Canberra Times*, 27 July 2019, online.

[8] Jessica Kidd, 'Intelligence on alleged meat grinder bomb plot came from Israel, Australia confirms', *ABC News*, 22 February 2018, online.

[9] Martin Callinan et al., *Defence and security R&D: a sovereign strategic advantage*, ASPI, Canberra, January 2019, online.

[10] List of participants: Australian Federal Police, Attorney-General's Department, Department of Defence, Government of South Australia, Office of National Intelligence, Department of Home Affairs, BAE Systems, Palantir, Basis Technology, Pivotal, AiGroup, Genix, Leidos, UNISYS, iapa, aiia, Teradata, Semantic Sciences, Carnegie Mellon University (Australia), Deakin University, eResearchSA, LaTrobe University, University of Adelaide, University of Technology Sydney, University of New South Wales, University of South Australia and Australian National University.

[11] Oracle, *What is innovation management?*, no date, online.

[12] Oracle, Build an innovation pipeline, no date, online.

[13] Gary P Pisano, 'The hard truth about innovative cultures', *Harvard Business Review*, January–February 2019, online.

Acronyms and abbreviations

AFP	Australian Federal Police
AML	anti-money-laundering
CLEIF	Commonwealth law enforcement innovation framework
CRC	cooperative research centre
D2D CRC	Data to Decisions Cooperative Research Centre
ICT	information and communications technology
MoU	memorandum of understanding
R&D	research and development

About the authors

Genevieve Feely is a researcher for the International Program, focusing on peacekeeping. Her research interests include multilateralism, peace operations and the responsibility to protect. She graduated from the University of Queensland in 2018 with a Bachelor of Arts/Bachelor of Laws, majoring in French and Peace and Conflict Studies. She is currently undertaking studies to be admitted as a lawyer.

John Coyne is the head of the North and Australia's Security program and the Strategic Policing and Law Enforcement program at ASPI**.**

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.

ORACLE®

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

About Strategic Insights

Strategic Insights are short studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

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

ISSN 1449-3993

Towards a Commonwealth law enforcement innovation framework