

Corruption Prevention Network Presentation
Lifting the Security Blankets:
New Technologies & Security – Changing Corruption Risks

Good afternoon. I'm here to talk about Corruption Risks and the effects of contemporary developments occurring in technology and security. However, I don't intend to talk directly about specific technologies – it's far too late in the day for that. Rather, I'm going to explore the role of corruption in the context of emerging threats at a national level and draw out several inter-related themes. My overarching theme today is the role of Public Sector Corruption as an enabler of serious and organised crime and potentially terrorism.

So let's do a little role-playing to set the scene.

How many of you have played The Sims or Sim City? Or maybe you'll only confess to having heard of this series of games, which allow players to develop their own real-life city. Let's imagine being a Sim Terrorist for a moment – planning and executing a terrorist attack on our Sim City, which is called Harold. We're going to blow up the Harold Harbour Bridge – what do we need?

[SLIDE – BRIDGE]

Firstly we need access to information about Harold and its environment to help reduce the risk of compromise. Ideally, our associates or friends currently residing in Harold can supply us with this. They would be able to tell us about:

- The easiest points and times of entry
- How to avoid detection or attention upon entry
- Where to stay
- Rendezvous points and times

How do we conceal our movements and whereabouts? We need

- a false passport
- access to non-traceable money, through setting up a false bank account or getting a false credit card
- we will probably also need multiple false identities as a contingency against possible compromise in case we are forced to abandon our plans or escape quickly.

We'll also need flight tickets - return of course. Maybe we should confuse the authorities by arriving and departing several times under various identities to complicate our movements and travel history. In any event, we will definitely need secure lines of communication with our bosses – or perhaps we should meet face to face to minimise the

risk of any technologically savvy law enforcement types eavesdropping on our discussions.

Now, would we rather use high quality forged documents or the real McCoy that will withstand scrutiny by the Police, with back up data entries and legitimate histories on Government databases. To get those you need either to fool someone on the inside or corrupt them – mmmmmm risky.

How do we recruit such a person? Find someone sympathetic to our cause? But how do we find them – we can't exactly just put an ad in the paper. Use friends of friends? How about we simply threaten someone or use blackmail? That would be very risky for this job, but these are all possible options. Luckily we have a pre-arranged solution – a member of our organisation infiltrated a key public sector organisation in Harold years ago. No one will suspect her!

Once in Harold we'll need to stay with our friends for a few days to familiarise ourselves with our new environment and decide where to live, for how long and if we want to stay in one place or move around. Renting can be problematic of course – some letting agents ask too many questions and want reference documents – so we'll try and avoid them if we can. We might initially take a sub-let if we can find one, that's much less hassle.

Will we take a job? That will provide us with a great reference point. What about student life? Maybe enrol into an Australian History course at the University of Harold and just blend in (in my case as a mature age student!). How do we get in though? Possibly on a false ID or with our false papers.

How will we communicate with our colleagues here in Harold City? We probably need to get a mobile phone so we can communicate. We'll have to produce ID documents to at least the 100-point standard if we do that. It might be easier to get a stolen phone. A potential problem is that telecommunications carriers are improving their technology to locate and disable stolen mobiles. Never mind, we can always fall back on the good old public phone box.

Finances now. Can't blow up a bridge just like that, especially Harold Harbour Bridge – it's very, very big. We'll need funds to buy munitions and explosives, a place to build and hide things and, of course, we have to organise our logistics. We need to set up a bank account in a false ID to organise and transact funds. We'll use cash wherever possible, but someone will need to get through the 100-point test – with our network and fake ID's that should be pretty easy. We won't be ripping off anyone so we should not attract too much attention from the regulators.

What about our transport? This is a high-risk area. We need to get around easily and quickly and the flexibility of our own wheels is tempting, but what about registration, insurance and a licence? We have 3 choices:

- Use a re-birthed car. It's a bit risky for our day-to-day run around – maybe we could reconsider this option if we need to use a car bomb.
- Use a friend's car. This is OK if we don't like our friend and he/she doesn't know who we really are. Still, an unnecessary risk of compromise here.
- Buy and register a second hand car with our false ID. Definitely the lowest risk option. Best to buy for cash from an auction and use our fake ID's at the RTA to bypass any problems.

What about the job at hand – the bridge itself. We know a little about engineering but this is a big bridge. Where are its weak points? How much explosive will be needed to bring about critical structural failure? What type of explosive charge will be best? How can we conceal it and for how long? What's the best way of achieving detonation (A mobile phone was used in Bali)? How do we minimise the risk of detection while placing the charge/charges? We need intelligence and

information to answer these questions. At a minimum, we'll need inside information on:

- the bridge's structure
- what time of day and what day of the week blowing the bridge up will have maximum impact
- the location of CCTV cameras
- whether the cameras are monitored and recorded
- whether the cameras generate electronic alarms
- security patrols
- how long could we safely leave the explosives hidden on a timer without their being discovered or if remote detonation is best.

Luck's a fortune – another one of our friends obtained a job as a security guard with the firm who protect Harold Harbour Bridge six months ago. So, getting up to date intelligence is easy.

The biggest risk in this operation is probably collecting and collating the explosives. How can we get plastics into the country? Not in our luggage that's for sure. Homemade bombs are easy to build and everything we need is here in Harold City. We just need plenty of ingredients and a lot of space to assemble it all. If we go that way we will definitely be using a vehicle. I think we're slowly covering the bases here, reducing the risk of our being detected, maximising the

chance of success and escape. By the time the various agencies react we'll be on a Qantas flight out of Harold city never to return.

Well, that's one scenario relating to a Bridge. I acknowledge that corrupt acts mostly occur as a one-off or entrepreneurial act. But as the risk of terrorist activity in Australia increases so too does the risk of corruption being used by terrorists groups. And there is no doubt that a number Public Sector organisations and employees are potential players in this complex web.

[NEW SLIDE – THREE KEY POINTS]

Today I want to talk briefly about corruption itself and its link to three of the emerging threats within the NSW Public Sector:

- Identity Crime and the value of information
- Critical government infrastructure
- Increasing reliance on technology

Having assessed the emerging picture I'll then try and assess the implications for the ICAC and explain how we are positioning ourselves for the future.

Corruption

Of all the offences and crimes I have investigated – and there are a few – corruption poses unique challenges and has unusual characteristics which, in my view, set corruption investigations slightly aside from what I'd term mainstream criminal investigation. This difference revolves around the relationship between the corrupted, the corruptor and the “victim” (if I can be permitted to call an entity such as an organisation a victim).

To begin let's quickly remind ourselves about some long-standing paradigms, which still hold true. People commit corrupt acts for a variety of reasons and in a variety of ways. Greed is the most common reason, and the acts can include bribery, deception, fraud, misappropriation or theft of property, forgery and other forms of gaining an illicit pecuniary advantage. Let's not also forget that fear and coercion may occasionally be the driving factor, as opposed to greed, including through blackmail or threats. Political or religious affiliations may also be drivers – look back to McClean, Philby and Co or to current day religious fundamentalism. Corruption is as old as society itself and thrives in a climate of high autonomy and low supervision.

So, let's look at the role of the corruptor and his or her relationship with the corrupted. How do corruptors select and identify potentially corrupt officials (including colleagues) – or is it the other way round? Put yourself in the shoes of a corruptor who needs a 'favour'. Would you make a 'cold' approach to someone, or prefer to rely upon approaching someone you know, or use a friend's recommendation or introduction. Bear in mind that corruption need not always be motivated by the entrepreneurial spirit and need not involve financial transactions.

Corruption and fraud are of course close cousins; fraud may often involve an element of corruption and corruption may often involve a fraud, or series of frauds being committed. This interrelationship is somewhat reflected in the composition of my Investigation Teams at the ICAC, where specialist fraud and financial investigators work alongside criminal investigators.

In general, both Fraud and Corruption offences have many similarities. They are both insidious, sneaky and take advantage of weaknesses in systems or people. They often leave little forensic evidence for the crime scene examiner to find, have little in the way of eyewitness evidence, are perpetrated against or by an employee or insider and are generally motivated by greed.

I accidentally stumbled upon the link between fraud and corruption when, in 1997, I was first approached to help establish a new Anti Corruption Squad in the London Metropolitan Police, having for 15 years previous been entirely inclined towards investigating organised crime and terrorism.

One of the more interesting jobs I worked on involved the UK Customs Service, who asked us to investigate the National Crime Squad, as they believed their operations were being compromised by a corrupt NCS Officer. In fact we discovered that the 'leak' was a Customs Insider, a clerk. We targeted Jimmy the 'Turk' or Jimmy the 'Hit man' – a colourful criminal who drove around in a \$500,000 Bentley. Jimmy was actively involved in the drug trade and hard to catch. We set up a sting against the clerk and created a false operation onto the Customs database, which our clerk obligingly leaked to Jimmy. Our methods were highly covert and I won't go into them here, but apart from leaking details about the false job, the clerk also leaked information about a fictitious informant. This led to Jimmy going into a frenzy trying to work out who 'Wilberforce' was and when he seemed to be about to accuse someone we had to remove that person to witness protection. Worryingly, Jimmy also had details of home addresses and bank account details of some of the customs investigators. He was also prepared to plan and arrange for the Customs Office to be broken into to remove evidence against him. This clerk wasn't making a mint – he

was scared and felt cornered by Jimmy. In the end he gave evidence and needed protection.

The relationship between crime, organised crime and terrorism, and the role of public sector employees as potential enablers is of particular interest to me. In 1989, the then Chairman of the NCA, Peter Faris QC, addressed the Fourth International Anti-Corruption Conference and argued that corruption was not ‘fundamental’ to organised crime, in so far as organised crime could exist without it, but acknowledged it was often a central element of organised crime. Mr Faris noted:

“Corruption will play a central part in an organised criminal enterprise where it is required to allow the illegal market in question to operate smoothly”.

In other words, corruption may at times be necessary either to facilitate the actual perpetration of a crime or as a means of avoiding detection. In saying this I draw no distinction between criminals and terrorists.

Identity Crime

[NEW SLIDE – HOLY GRAIL]

A recent National Criminal Intelligence Service (UK) report identified important links between ID fraud and organised crime and adjudged corruption to play a supporting role. There are however some gaps in the Intelligence picture, for example, although forgery and counterfeiting are clearly the most prevalent methods used to create false documents, the role of corrupt officials and employees turning a blind eye or worse still providing false documentation is not as well documented. Corruption of insiders give identity thieves and fraudsters potential access to the Holy Grail - seemingly bona fide ID documents which will stand up to scrutiny and are backed up by data entries on internal Government data bases.

I'll give another example from a recent Canadian paper entitled *Identity Fraud and Transnational Crime*, by Juan Gabriel Ronderos. Mr Ronderos suggests that corruption plays a significant role in many false identity schemes and that the role of various corrupt officials must be acknowledged. Mr Ronderos says that Immigration Officers and Police Officers at points of entry are particularly vulnerable to involvement in criminal schemes, and he provides details about allegations of consular officers selling Canadian Visas. He also cites

the conviction of a former immigration judge for his role in aiding illegal immigration as providing sufficient evidence upon which to base these concerns. This targeting of officials may be more widespread.

This year the UK Home Office published the findings of a study by Joel Miller into Police Corruption in the UK. Miller came up with some interesting and relevant findings. Firstly, that information compromise was the single most common type of corrupt activity. Information can be obtained for personal purposes, passing information to friends and associates, leaks to the media and leaks to criminals. Reasons for insiders being targeted by organised crime included their access to the data source and low levels of managerial and audit supervision. Miller also found that leaked information even found its way to criminals when it wasn't deliberately intended to, being passed through associates, relatives, friends and social acquaintances. So the official can not only facilitate the crime but give access to information and intelligence.

Consider for a moment the break-in this week at the Department of Transport in Canberra, thieves using a swipe card to enter the security area to swipe a laptop upon which was stored sensitive data. It was said by one observer "they must have known what they were doing" Last week at the Customs offices near Sydney airport, more sensitive data

stolen. Just stabs in the dark, or based on accurate and reliable information? I'll leave you to ponder the issues.

So we can see that some information and data can be extremely valuable. The trick is to work out what information exists, where it is and its value to criminals. Just working out what's publicly available and what isn't is very difficult due to the proliferation of open data sources and Freedom of Information.

The link between terrorism/ID fraud/corruption has been recognised by others, for example the UK Home Office have sought to disrupt the use of ID fraud by organised criminals and terrorists through the introduction of new legislation. Identity fraud was also identified as being a priority in the Commonwealth and States and Territories Agreement on terrorism and Multi-Jurisdictional Crime in April last year.

Critical government infrastructure

So let's talk about Terrorism for a moment. The relevance of its link with corruption was brought home to me quite some time ago, during the mid 90's in London, whilst I was at the Anti Terrorist Branch. An Active Service Unit (ASU) of the Provisional Irish Republican Army (PIRA) had established themselves for many months on the mainland

of Britain, assimilating themselves covertly, unnoticed and undetected into mainland Britain, renting property, buying and driving motor vehicles, working, socialising, shopping and in the meantime gathering intelligence about their primary targets, planning, contingency planning and building the logistics required to support an attack and a stockpile of necessary arms.

This particular ASU intended launching an attack against critical government infrastructure, a tactic regularly employed then by the PIRA in order to achieve maximum economic pressure whilst maintaining a low body count in order to keep ‘on side’ with beneficiaries abroad. They had been instructed to attack London’s power supply.

[NEW SLIDE – IRA HEADLINE]

This required geographical knowledge, technical knowledge and knowledge about security measures. A large number of powerful electricity sub stations exist around the outskirts of London. In deciding which ones to blow up it was necessary to identify those that would wreak the most lasting and serious damage upon the National Grid around London. They chose well - very well - and the impact, should they have been successful – if we hadn’t been watching them –

would have plunged London into darkness for days and caused blackouts on a huge scale that would have continued for months.

I wonder how many public sector agencies they may have come into contact with during that time. One thing is certain – in order to achieve their objectives they required intelligence. Sources of intelligence can of course be various, the most effective often being ‘agents’, or ‘insiders’, and, of course ‘reconnaissance’ or surveillance. Those of you with an investigative background will appreciate the value of covertly obtained, accurate and reliable source information.

Infrastructure provides terrorists with a target for achieving maximum economical damage, environmental damage or deaths. Power supply, water supply, fuel supply, lines of communications, transport infrastructure and public buildings often fall under the custodianship of Government Agencies or Private Sector Organisations who are bound to Governments through partnerships, contracts and/or legislation.

Public or private, the message is the same; we all rely upon these services in the conduct of our everyday lives and to provide us with a quality of life. In NSW many of these services are within the domain of the public sector, and as such within the ICAC operating environment. In the context of critical infrastructure, recent events spring readily to mind, like the Blackout in the USA a little earlier this year. We won't

speculate about the precise cause of that particular incident, as it's almost academic for our purposes. What that incident demonstrated was the frailty of a key piece of infrastructure and its ability to seriously impact upon the lives of millions of people. If a power failure in one minor part of the system, and this goes back to my little anecdote about the PIRA, can lead to such a catastrophic failure of nearly half the power grid in the USA, then imagine what a knowledgeable and determined terrorist group could achieve.

The potential benefits for criminals and terrorists from our critical infrastructure should not be under-estimated, nor should the role for corruption as a means of acquiring intelligence – about collection and storage points, distribution networks, underlying technologies, weaknesses and vulnerabilities and security arrangements. Much of this information may of course already be a matter of public record, but my point is that intelligence and information is valuable and there is a market for it.

Use of technology

What then of the effect of advances in technology? As the costs and access to advanced technology becomes easier, facilitating the production of false documents, through advanced desktop publishing and digital technologies, governments will probably respond in kind

through improving legislation, policy and security systems. In fact, this is already happening in the aftermath of September 11 and the Bali bombing. Concurrently, government agencies are also utilising advanced web based technology to improve service provision and aggregating information in 'data warehouses', using technological advances to improve security and using IP systems as a means of communicating and data sharing with clients and partners. These initiatives make the use of an insider to create false data or to obtain data illegally, without the need to defeat firewalls or risk using forged documents, an increasingly attractive option for many criminals.

[NEW SLIDE – DISORGANISED CRIME]

But whatever countermeasures governments and agencies dream up, rest assured that criminals and terrorists will adapt and evolve accordingly. Criminal networks can be very complex and stretch over continents. Traditional views of the organisation of criminal and terrorist groups no longer apply. What is clear is that such groups are resilient and adaptive, based upon loose and fluid organisational structures and this makes them formidable opponents. Peter Klerks, a Dutch academic, has examined the social networks of organised crime gangs and suggests that these groups do not structure themselves in a conventional sense, and as a result they are fluid, able to improvise, innovate, adapt and avoid detection – disorganised crime might be a

more appropriate tag. Additionally, such groups are networked and the previous ethnic homogeneity of many criminal groups is now largely a thing of the past, presenting real challenges for law enforcement.

As you are aware, the proportion of fraud involving identity crime is rapidly on the increase due, mainly, to this proliferation of technology. Fraud is now one of the fastest growing crimes in Australia and is estimated to be valued at up to \$5 billion per year, Australia-wide, while ID fraud alone is believed to account for \$2 Billion.

So the motivation for sophisticated criminals and terrorists to target such information and data continues to grow. The threat of cyber crime and even cyber terrorism is also going to grow as information is increasingly stored and aggregated as data, requiring increasingly sophisticated electronic security measures. In the UK local elections this year, people could vote on line. I'm given to understand that it is hoped to extend this to Australia for the next Federal Election. This is of course the central pillar of our democratic society and I won't even begin to assess the security implications. Suffice to say, no doubt there are some worried tech heads out there somewhere hoping they can protect the integrity of such systems.

Even Bill Gates takes a hit every now and then – the recent blaster worm virus is an example of what one could term an almost frivolous crime with global ramifications.

As technology, legislation and corruption resistance methods evolve, so too does corruption itself. Corruption and many other forms of crime, particularly what we term organised crime, mutate over time. As with many crimes, when law enforcement has some success in prevention and detection, the perpetrators change their methodology and tactics or worse still totally reinvent the wheel. Certainly the average criminal has the ability to be far more adaptive and flexible than any system designed to prevent and catch them engaging in their enterprises.

Of particular interest to us today is the role of the ‘insider’, the person who is the conduit between the ‘assets’ of an organisation, and the outside world or (black) market place. I am of the view that as governments move increasingly towards e-government and data warehousing, their security arrangements will necessarily improve. In fact, advanced technologies such as firewalls, encryption, digital certificates, VPN’s, smart card and biometric access control devices are now becoming commonplace in the pantheon of government security. These technologies, combined with the increasingly sophisticated technical eavesdropping methods employed by

governments, will increasingly push criminals away from a reliance upon technology as a means of facilitating their crimes and towards targeting and using insiders as ‘Trojan Horses’ as a means of avoiding detection and accessing whatever service it is they require.

This has implications for us all. Increasingly sophisticated enforcement and collaboration between agencies and countries, advances in technology and communication and the globalisation of criminal enterprises has moved the boundaries beyond recognition. Where does the line between organised crime and terrorism exist? How do we differentiate between the enablers of crime, organised crime and terrorism? Can we look at one specific type of crime in one sector in isolation from others? How do we map out jurisdictional overlaps and gaps? These are not questions with easy answers. Add to this a picture of proliferating technological developments in intelligence gathering techniques, improving prevention initiatives and the fact that many countries are increasing their security measures through legislative and other advances such as biometrics.

ICAC Perspective

One of the key challenges we face at the ICAC is understanding and predicting corruption risks facing the NSW Public Sector. To do this it is necessary first to have a contemporary understanding of the nature of

corruption, next to understand the relationship between that sector and the world at large and finally to understand the issues which are particular to the NSW Public Sector, or the ICAC operating environment. In other words we can't begin to understand what's happening on the ground unless we look at problems from a more global level, and vice versa. Therein lies a key challenge for many Intelligence professionals – convincing people of the importance of the big picture when looking at specific issues and producing an intelligence product with relevance and impact.

The establishment of an effective Strategic Intelligence function is something that we, like so many other organisations, aspire to and we are making some good in-roads in that direction. We are lucky in that we not only have an investigative function but also a Corruption Prevention/Research and Education Division where there exists a wealth of knowledge and expertise. Of course, I like many investigators will, if let off the lead, go chasing after the evidence to get the collar. In doing so I may leave in my wake a trail of destruction and missed opportunities outside the evidentiary sphere. Weaving together investigative skill, knowledge and methodology with a corruption prevention focus allows us to look at issues in the round, maximising outcomes and deterrents.

Of course, corruption comes in various guises and I'm not here to tell you that all corrupt acts are linked to a higher or more sinister purpose, nor am I here to tell you that every public sector employee or agency presents high levels or the same levels of risk. But I do believe that developments at a National and International level may reasonably be expected to impact upon many of the people and organisations populating the NSW Public Sector, including of course the ICAC.

Conclusion

The ICAC is already assessing many emerging corruption risks, some of which relate to technology and security, and these include the proliferation of identity crime, the growing terrorist threat in Australia and the increasing reliance of organisations upon information technology for processing and recording data.

The relationship between crime and identity crime is based upon the need for criminals to dishonestly obtain money or property whilst removing the ability of law enforcement to link the offender with the crime. If criminals see corruption as being the most effective and efficient means of achieving this then they will seek to do so.

The ICAC is improving its relationship with other investigative agencies and is working more closely, where possible with other

agencies in either joint taskforce arrangements or through sharing information and intelligence. In this way we can achieve our own sector level objectives whilst contributing to the prevention of organised crime and terrorism. It is my hope that the agencies and employees of agencies in the NSW Public Sector understand the importance of their assets, including their knowledge and information, and that by applying appropriate corruption resistance and security programmes they too are able help in making our sector a hard target for crime and terrorism.