Organised crime in Australia has received increased attention over the last decade, with the enactment of legislation and the development of other interventions that have sought to control this serious criminal phenomenon. Although the success of such interventions in reducing organised crime is yet to be subject to detailed evaluation, prior research has identified certain risks associated with policy responses that could, arguably, also lead to counterproductive consequences (Guerette & Bowers 2009; Smith, Wolanin & Worthington 2003). One consequence of enhanced legislation and/or law enforcement approaches developed to combat organised crime is so-called ‘tactical crime displacement’, namely that criminals may modify their tactics in order to circumvent the effects of new legislation or increased law enforcement activity, thus allowing them to continue to offend with a reduced risk of detection or criminal justice action taking place. One particular risk of tactical crime displacement is the potential for organised crime groups to focus more on forming corrupt relationships with public officials in order to obtain information that minimises the risk of detection and prosecution.

This paper illustrates how organised criminal groups can alter their patterns of offending by inducing public officials into corruptly disclosing information relevant to the facilitation of further criminal activity. This process of corruption is explained using the notion of ‘crime scripts’, as developed by Cornish (1994), and the 5i’s crime prevention framework developed by Ekblom (2011). Making use of public-source information about the commission of such crimes, as exemplified in two recent corruption cases, some intervention strategies are proposed that may be effective in reducing the risks of corruption of public sector officials by organised crime groups in Australia.

Organised crime and public sector corruption: A crime scripts analysis of tactical displacement risks

Elizabeth Rowe, Tabor Akman, Russell G Smith and Adam M Tomison

International context

The United Nations Convention Against Transnational Organized Crime (UNTOC) is the primary international instrument dedicated to combating organised crime. For present purposes, organised crime will be defined in accordance with article 2 of UNTOC (UN 2004a), which is also the definition adopted by Australian law enforcement and government agencies following the Convention’s ratification in 2004, namely:
a structured group of three or more
persons, existing for a period of time,
acting in concert with the aim of
committing serious criminal offences in
order to obtain financial or material benefit
[where];

a serious crime is defined as an offence
punishable by at least four years’
imprisonment; and

a structured group is one that is not
randomly formed, but has some existing
internal structure and exists for some
period of time before and after the
commission of an offence.

The United Nations Convention Against
Corruption (UNCAC) (UN 2004b) outlines
the actions that amount to corruption from
an international perspective. These include,
but are not limited to, bribery of national
public officials, abuse of functions and
power, using office for personal gain and
any actions that violate the interests of the
public (UN 2004b).

Although organised crime and corruption
are dealt with in separate UN Conventions,
they are not completely independent
criminal phenomena. Prior research has
found a strong association between public
sector corruption and organised crime
groups (Buscaglia & van Dijk 2004). For
example, groups involved in human
trafficking and people smuggling frequently
seek to corrupt border and customs officials
to facilitate cross-border trafficking
operations (Holmes 2007). In addition, both
theoretical and applied research has found
that corruption is a key tool in the arsenal of
organised crime groups (Sukharenko 2004;
Vander Beken 2004).

Organised crime and
corruption in Australia
Organised crime

The threat posed by organised crime in
Australia is considered so great that
legislation has been passed that aims to
proscribe and penalise criminal activities and
to regulate industries that could facilitate
criminal activity (see below). Outlaw
motorcycle gangs (OMCGs), motorcycle
clubs or groups whose members use their
clubs as conduits for criminal enterprises
(Loucusic 2002), are the most recognised
form of organised criminal enterprise in
Australia (Holmes 2007). Alongside the
highly visible OMCGs, there are also
ethnic-based crime groups, family-based
crime groups and groups formed on the
basis of place of origin such as prisons
(CCC WA 2005). The primary organised
criminal activity in which these groups are
involved is illicit drug trafficking, however,
criminal syndicates also engage in money
laundering and financial crime to further
expand and to legitimise their criminal
organisations (ACC 2011).

Criminal organisations in Australia
are networks of criminals varying in
sophistication, which have highly flexible
structures and modes of operation (ACC
2011). These organisations have the ability
to infiltrate a wide range of industries and
markets, while adapting to changing
opportunities, economies and technologies,
all in order to increase their profits (ACC
2011). For this reason, these networks
contribute to a large proportion of serious
crime in Australia (ACC 2011).

Organised crime in Australia can have a
negative effect on the economy by affecting
legitimate businesses’ access to resources,
reducing tax revenue and increasing costs
to the criminal justice system (ACC 2011).

Organised crime in Australia is between $10b and $15b a year, the estimated cost of organised crime in
Australia is considered so great that
the threat posed by organised crime
in Australia is between $10b and $15b a year,
the estimated cost of organised crime in
Australia (ACC 2011).

In recent history, there have been some
highly publicised instances of official
corruption with links to organised crime
groups. The operation also included the covert surveillance of a Police General Support Intelligence Analyst.

Covert surveillance and IT audit logs captured the Police Analyst accessing the controlled intelligence report via
privileges on the police computer system. He was observed reading the report on his screen and then printing the report before
reading it again. He then made a telephone call while viewing the report.

On 10 November, police became aware that a person believed to be heavily involved in illegal drug distribution, was aware
of information specific to an intelligence report released on 5 November. Examination of telephone records showed the
dealer, his brother and the Police Analyst’s cousin had had contact.

Between 17 November and 15 December, officers of the Professional Standards Command released another two
targeted intelligence reports, one regarding an illegal poker night involving members of the OMCG, to which the Police
Analyst had also been invited. Once again, covert surveillance observed him accessing and printing the intelligence report
before removing a section of the report and leaving the office. Later that day, he met his cousin and was observed having
a lengthy discussion. The exchange of an item was also observed.

On 16 December, search warrants were executed at the premises of the Police Analyst and his cousin. A number of
items were seized including an internal police computer system profile of a Person of Interest from the cousin’s
premises. Subsequent analysis of IT audit logs found that the Analyst had accessed and printed the same report as
that found in his cousin’s premises. Fingerprint analysis of the seized report found both the Analyst’s and his cousin’s
fingerprints on the report.

Box 1: Corrupt release of police intelligence reports

On 5 November 2009, law enforcement investigators made the first of several releases of controlled intelligence reports
onto the NSW Police computer system in order to determine if a staff member was corruptly passing on intelligence to
criminal contacts. The operation also included the covert surveillance of a Police General Support Intelligence Analyst.

Covert surveillance and IT audit logs captured the Police Analyst accessing the controlled intelligence report via
privileges on the police computer system. He was observed reading the report on his screen and then printing the report before
reading it again. He then made a telephone call while viewing the report.

An hour and 45 minutes later, the Analyst made a mobile telephone call to his cousin, a person known to associate with
an OMCG. During the course of this conversation, the Police Analyst made arrangements to meet his cousin that evening.

Before leaving for the meeting surveillance observed him removing pages—containing the narrative—of the report and
placing them in his briefcase.

On 10 November, police became aware that a person believed to be heavily involved in illegal drug distribution, was aware
of information specific to an intelligence report released on 5 November. Examination of telephone records showed the
dealer, his brother and the Police Analyst’s cousin had had contact.

Box 1

Corruption

The corruption of public officials in Australia
is often highly publicised as it violates the
notion of ‘public service’ through the
officials’ abuse of power and position.
However, little research has been carried
out in Australia regarding the link—if any—
between organised crime and corrupt public
officials. Yet corruption has been identified in
both the wider public sector and the criminal
justice system in particular (ACC 2011).

In recent history, there have been some
highly publicised instances of official
corruption with links to organised crime
groups (see Boxes 1 & 2). However,
compared with the international community,
Australia has experienced a relatively small
amount of organised crime in this sphere
and there is little public-source evidence
to suggest that there is any large-scale
corruption of the public sector by criminal
organisations (Gilligan & Bowman 2007).

Despite this, there is, arguably, an ongoing
risk of corruption of public servants by
criminal organisations. One reason for
this lies in the impediments that have been
to the commission of organised
crime through the use of more intensive
legislation and the development of
coordinated law enforcement activities.
Box 2 Corrupt facilitation of drug trafficking

Between 2006 and 2008, the former Assistant Director Investigations at the NSW Crime Commission became involved with a drug trafficking organisation and the importation of 300kg of pseudoephedrine. At the time of his arrest, he had been with the NSW Crime Commission for 12 years ([2011] NSW Supreme Court 1422, 8 December 2011).

The criminal enterprise was suspected to have begun when the Crime Commission investigator became friends with a known international drug trafficker with connections to money laundering operations. Following his arrest for related offences, the drug trafficker acted as an informant to the Crime Commission with the former Assistant Director Investigations being one of his handlers ([2011] NSW Supreme Court 1422, 8 December 2011).

The former Assistant Director Investigations began his criminal activities when he entered into an agreement with his informant and a legitimate businessman to import a large quantity of pseudoephedrine concealed in a container of rice, which was being sent to the food importing and distribution business run by the business associate. The informant’s connections with Dutch organised crime syndicates were used to access the illegal substances ([2011] NSW Supreme Court 1422, 8 December 2011).

The former Assistant Director Investigations’ motivations for becoming involved in the criminal organisation were clearly financial gain, to clear himself of his debts and to provide for his family. It is believed that these debts may have been a result of a mortgage and his wife’s psychological and health problems (alcoholism). There was also an indication of his excessive spending in which he bought his mistress expensive gifts and took lavish holidays. However, the money received from the criminal enterprise was far beyond the amount needed to satisfy these expenses ([2011] NSW Supreme Court 1422, 8 December 2011).

Throughout the investigation into his conduct, he was recorded using his professional knowledge and experience to advise the businessman on the steps to take to lessen the risk of the criminal organisation being detected. Specifically, he advised on what law enforcement procedures would be used in relation to the shipment. Using his personal contacts made through his position, he made enquiries about the status of a shipment of rice and whether it had come to the attention of Customs, reporting his findings to the businessman. The investigation also uncovered several email communications between the informant and the accused illustrating his key role in the trafficking of the substances ([2011] NSW Supreme Court 1422, 8 December 2011).

The former Assistant Director Investigations had corruptly advised his conspirators and had used the resources available to him to further facilitate the criminal enterprise. He was charged with three offences in 2008:

1) conspiring to import;
2) knowingly taking part in the supply of a large commercial quantity of prohibited drugs; and
3) conspiring to pervert the course of justice.

In December 2011, he was found guilty of all three charges and sentenced to 22 years imprisonment with a non-parole period of 16 years ([2011] NSW Supreme Court 1422, 8 December 2011).

If these measures make crime too difficult to commit using conventional approaches, it is arguable that organised criminals may look to alternate means, such as the corruption of public servants as an effective way of gathering the information and resources needed to continue their patterns of offending unabated. Public servants are important gatekeepers of information critical to the commission of serious crime, such as personal identity information, as well as strategic police intelligence on how organised crime is being investigated and monitored. Obtaining this information from insiders is an efficient means of planning a major criminal enterprise.

Australian legislation and interventions

Anti-money laundering legislation in Australia was developed as a response to two Royal Commissions in the 1980s, which exposed links between money laundering and organised crime—particularly major tax evasion and fraud. The Financial Transactions Reports Act 1988 (Cth) (FTR Act) was the first piece of legislation in Australia that focused on preventing and detecting money laundering. The FTR Act required various financial entities to report suspicious transactions, transactions over a certain financial level and transactions going overseas. In 2006, the Anti-money Laundering and Counter Terrorism Financing Act 2006 (Cth) (AML/CTF Act) replaced the FTR Act, extending regulatory controls to alternative remittance providers, due to the concern that these systems could be abused to facilitate money laundering, organised crime and the financing of terrorism.

In addition to these preventive measures, stolen asset recovery mechanisms also exist in Australia. The Commonwealth confiscation of assets regime is contained in the Proceeds of Crime Act 2002 (Cth) (POCA 2002), which allows law enforcement to pursue the recovery of assets linked to an offence after a conviction. POCA 2002 also allows civil recovery of assets, such that assets suspected of criminal origins are able to be seized without the necessity of a criminal conviction. POCA 2002 is designed to prevent the laundering of illegal profits made by organised crime groups, which will further prevent engagement in criminal activities by these groups. Each state and territory in Australia also has comparable versions of organised crime-related legislation.

Displacement risks

Crime control initiatives, such as those outlined above, can cause crime displacement by triggering changes in the location, time, target, offence tactic or offender (Guerette & Bowers 2009).

Crime displacement can be:

• temporal—(ie offenders alter the time at which they commit the offence);
• spatial—(ie offenders change the location of their offending);
• target—(ie offenders switch from one target to another);
• tactical—(ie offenders use different methods to carry out their crimes);
• offence—(ie offenders switch from one crime type to another); and
• offender—(ie new offenders replace existing offenders) (Guerette & Bowers 2009).

If legislation is effective in preventing organised criminal activities, crime displacement may occur. There have been few evaluations or other research conducted into displacement effects of organised crime prevention initiatives, with Levi and Maguire (2004) acknowledging that displacement as a result of organised crime prevention initiatives would be difficult to measure, despite evidence suggesting that displacement is occurring. This difficulty arises from the absence of a universal definition of organised crime and the nature of such criminal organisations, which are ‘underground’ or covert by nature and therefore hidden (Levi & Maguire 2004).

Further, while displacement research typically examines street crimes, such as burglary and motor vehicle crime, organised crime by its nature is complex, taking place across different locations and times, and involving multiple offenders. Thus, spatial, temporal, offence and offender displacement may not be a major consequence of attempts to prevent organised crime because these factors are changing continuously, subject to the illegal and legal markets and the profit-driven nature of criminal organisations.
However, there is some evidence for tactical displacement as a consequence of e-crime prevention techniques (Smith, Wolanin & Worthington 2003). It has been suggested that hardening electronic targets would motivate offenders to seek alternative means of performing their criminal activities by gaining access to the information they seek through internal agency sources, using methods such as corruption and infiltration. This is of relevance to the current discussion as cybercrime and the use of technology is a developing and increasingly used technique within criminal organisations (ACC 2011; and see further discussion below).

The emerging risk of ICT and corruption

The use of information and communications technologies (ICT) in connection with corruption has been identified as an ongoing threat to the public sector in two broad ways (Smith & Jorna 2011). First, ICT may be the target or object of the offending; and second, ICT may be used as a tool for offending (Choo, Smith and McCusker 2007). Of particular interest is the ability of organised crime groups to use ICT to assist in the corruption of individuals in the public sector. Research into the area of ICT and organised crime shows that a significant number of external breaches of data can be attributed to organised crime syndicates (Verizon & United States Secret Service 2011). According to the 2011 Verizon Data Breach Investigations Report, external agents accounted for 92 percent of data breaches and 58 percent of these were attributed to organised criminal groups.

Organised crime groups can use ICT as a tool to access personal information of employees in the public sector, enhancing their ability to coerce individuals into behaving corruptly (eg identifying financial hardships, important contacts that might be exploited, or other personal and family vulnerabilities). In addition to ICT being used as a tool to access personal information illegally, the widespread presence of social networking sites (SNS) has enabled people to publish a significant amount of personal information electronically. Sensitive information can be found on SNS, such as nicknames and other information that can assist criminals to undertake more refined research on targets. Once a person’s name, job title and profession are discovered, address and phone numbers can be found from online directories. This information, when combined with information collected illegally and a number of other open sources of information, allows comprehensive dossiers to be developed (Hart 2010).

Further, the information available to organised crime groups is not only limited to sources available online. ICT-facilitated methods can be used in conjunction with more traditional methods, such as sifting through rubbish, which has the potential to generate vast amounts of personal information and that may be enough to coerce or to induce an individual into offending. An Australian example of a public official being corrupted by organised criminals is provided in Box 2, with the role that ICT played in the acts of corruption explored in Table 1. In light of this discussion on tactical displacement and e-crime, it seems reasonable to contend that the adoption of ICT as a means of corrupting public officials may increase and be associated with the introduction and enhancements of legislation and regulatory controls implemented in Australia to prevent and deter traditional organised crime activities.

Situational crime prevention and crime scripts

Understanding how organised crime groups may attempt to coerce public servants into disclosing information is a key element in its prevention. The benefit of taking a situational approach is the ability to focus on the goals and modus operandi of organised crime groups, rather than attempting to understand individuals and their criminality (Cornish & Clarke 2002). Reducing opportunities for crime is a complementary strategy to targeting offenders and may be more efficient overall. Once goals and methods are known, the next step is to develop techniques to prevent, constrain or disrupt the criminal activity. These need to be specifically tailored to the criminal acts and therefore require a detailed understanding of the whole process through which the crime is commissioned and then takes place (Cornish 1994). Research of this kind has already been undertaken in relation to the resale of stolen vehicles (Tremblay, Talon & Hurley 2001) and cheque forgery (Lacoste & Tremblay 2003).

To obtain an understanding of the crime commission process, Cornish (1994) argued that crimes can be examined through the use of crime scripts. Scripts are a sequence of ‘script functions’ and accompanying ‘script actions’ that organise our knowledge and understanding of routine behavioural processes (Cornish 1994: 161). For example, eating at a restaurant involves more than just eating; it requires deciding which restaurant to eat at, entering the restaurant, choosing a table, ordering, waiting, eating, paying the bill and leaving (Cornish & Clarke 2002). Similarly, the commission of a crime or the coercion or inducement of a third party to commit a crime can be broken down into a number of routine processes. These include—preconditions, initiation, actualisation, doing and post-conditions, and these script functions have corresponding script actions (Cornish 1994). By developing an understanding of how organised crime groups may try to coerce or induce public servants, a script analysis can then be used to identify the script functions and corresponding actions. In Table 1, a script analysis is provided of the corruption of the Police Investigator’s activities described in Box 2. The information gathered through this process can then be put to use in preventing such activities.

Ekblom’s 5Is framework

Once crime scripts have been developed, it is possible to address crime risks through the development of situational crime prevention initiatives (although crime scripts analysis may also inform conventional offender-focused investigations as well as the disruption of offending). Such an approach should also form part of the general processes of risk identification and management outlined in organisational principles of risk management that government agencies and business now adopt (Standards Australia 2009).

The crime prevention process should not, however, be over-simplified or there may be a risk of overlooking key strategies or implementing ineffective and costly initiatives. A systematic and evidence-based approach is required. One such approach is the 5Is framework developed by Paul Ekblom (2011). This approach aims to provide crime prevention practitioners...
Involvement and Impact:

Intelligence, Intervention, Implementation, the 5Is approach is framed around a

oriented crime prevention methods.

across a range of situational and offender-

methodology for implementing initiatives

with an evidence-based framework and

resources available, the organisation and the

risk posed. The 5Is approach is a detailed

systematic approach to crime prevention,

which is explained more fully at


and Maguire (2004) have also applied the

approach specifically to the commission of

organised crime.

The specific methodologies used at each

of the five stages are dependent upon the

The Intelligence stage, carried out in part

through the crime scripts analysis described

above, provides a greater understanding

of the sequences of choices, decisions and

actions of organised criminals. Additional

intelligence should also be gathered

alongside the completion of a script

analysis, including an attempt to identify

the factors within the environment and the

criminal organisation itself that promote or

may prevent criminal activity (Ekblom 2011).

This stage sets the foundations and informs

the subsequent four stages and ultimately

informs the effective implementation of a

strategy to prevent organised crime. With

a successful script analysis completed, key

points for intervention can be identified. For

present purposes, only the first three stages

of the 5Is framework will be examined

as these stages are the most relevant to

preventing organised crime activities that

entail corruption. Involvement is less relevant

to this specific case because the opportunities

that facilitate corruption within the police are

largely (though not exclusively) within the

<table>
<thead>
<tr>
<th><strong>Table 1 Crime scripts analysis in the corruption of the former Assistant Director Investigations at the NSW Crime Commission by a drug trafficker</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Script function</strong> (Cornish 1994:161)</td>
</tr>
<tr>
<td>Preparation (establishing network of contacts and background information)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Pre-conditions (necessary preparatory acts)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Instrumental conditions (agreeing on initial acts to commence activity)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Instrumental initiation (essential preliminary research needed to execute activity)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Instrumental actualisation (first steps taken to commence criminal activity)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Doing (undertaking principal criminal acts)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Post-condition (procedures following commission of crime)</td>
</tr>
<tr>
<td>Exit (finalisation of criminal activity)</td>
</tr>
</tbody>
</table>

with an evidence-based framework and

methodology for implementing initiatives

across a range of situational and offender-

oriented crime prevention methods.

The 5Is approach is framed around a

sequence of tasks and steps, namely

Intelligence, Intervention, Implementation, Involvement and Impact:

• **Intelligence** is the process of collecting and analysing information. It should identify and develop understanding of the modus operandi of offenders and other relevant aspects of the crime. It should also generate understanding to support the other four elements of the 5Is approach.

• **Intervention** is about blocking, disrupting or diminishing the causes of the criminal event. For example, this may include removing the ability of organised crime to identify valuable public servant targets.

• **Implementation** is the conversion of intervention principles and methods into practice. This may require the input of resources to develop new practices or the development of new policies and procedures.

• **Involvement** requires the mobilisation of, and where appropriate, establishing partnerships with other agencies, departments or individuals. This should be led by the intelligence gathered at the first stage.

• **Impact** is the evaluation of the ultimate outcome, the intermediate outcomes and the process (Ekblom 2011).
control of the police themselves; that is, there are relatively few other external parties to involve. The prevention of corruption in other organisations (eg local government) will require greater attention to involvement activity.

An application of the first three stages in relation to organised crime and ICT as a tool for corruption is presented in Table 2. This analysis is, however, limited owing to the absence of currently available information on the motivations and tactics employed by organised crime groups in connection with the corruption of public officials. The interventions described in Table 2 are aimed primarily at decreasing the desirability of using ICT as a means of corruption. This would potentially be achieved through increasing the risks of detection associated with using ICT as a coercion method—one of the basic situational crime prevention elements identified by Clarke (1995). For example, implementing firewalls in computer and data systems and introducing surveillance systems in public officials’ offices and workspaces would be appropriate. Privacy implications of introducing ongoing surveillance of staff, however, need to be balanced with the level of risk of corruption, the impact of corruption on agency operations and the perceived crime prevention benefits that might occur against broader agency and human resources considerations. In the case described in Box 2 above, surveillance of communications was clearly considered to be appropriate in the circumstances.

SNS have also been highlighted as a potential information source for criminal organisations. The introduction of codes of conduct for using SNS and penalties for not adhering to these guidelines may be one strategy worthy of further consideration.

### Table 2 Application of the 5Is framework to the crime scripts analysis of the corruption of the former Assistant Director Investigations at the NSW Crime Commission

<table>
<thead>
<tr>
<th>Script action/intelligence</th>
<th>Intervention</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquire required IT equipment</td>
<td>Controlling dissemination of ICT</td>
<td>Registering names of buyers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Screening online transactions of high-risk individuals</td>
</tr>
<tr>
<td>Find possible information sources</td>
<td>Preventing outside access of personal details for public officials</td>
<td>Firewalls—computer and internet security on all personal devices</td>
</tr>
<tr>
<td></td>
<td>Limit the ability of informants and officials to form close friendships</td>
<td>Passwords</td>
</tr>
<tr>
<td></td>
<td>Limit the amount of employee information released to the public</td>
<td>Monitoring of handlers when contacting high-risk informants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reduce amount of specific information released to the media</td>
</tr>
<tr>
<td>Obtain possible target names</td>
<td>Limited release of names of investigations personnel</td>
<td>Withholding personal information and names from Internet site</td>
</tr>
<tr>
<td>Select target</td>
<td>Increase difficulty in accessing/making contact with public officials</td>
<td>Monitoring of handlers when contacting high-risk informants</td>
</tr>
<tr>
<td></td>
<td>Decrease the desirability of using public officials to facilitate criminal activities</td>
<td>Monitoring excessive lifestyle expenditure of officers</td>
</tr>
<tr>
<td>Research background of target for information or coercion or inducement</td>
<td>Reduce possible information sources on public officials</td>
<td>Limit use of SNS by public officials</td>
</tr>
<tr>
<td></td>
<td>Limit the ability of informants and officials forming close friendships</td>
<td>Limit dissemination of personal information on Web2 platforms (eg photos and names on SNS)</td>
</tr>
<tr>
<td>Contact target</td>
<td>Preventing contact through surveillance</td>
<td>Monitoring of handlers when contacting high-risk informants</td>
</tr>
<tr>
<td></td>
<td>Improve security within internal structures of the public sector regarding ICT</td>
<td>Education of public officials to detect and recognise corrupt behaviour</td>
</tr>
<tr>
<td>Use obtained information for coercion or inducement of target</td>
<td>Increase awareness of disincentives for colluding and rule setting</td>
<td>Anonymous hotlines for employees</td>
</tr>
<tr>
<td></td>
<td>Limit the ability of informants and officials having inappropriate contact</td>
<td>Workplace PC surveillance</td>
</tr>
<tr>
<td>Access information/induce behaviour/utilise corrupt official</td>
<td>Rule setting</td>
<td>Enhanced codes of conduct</td>
</tr>
<tr>
<td></td>
<td>Disincentives for corrupt behaviour</td>
<td>Workplace personal computer surveillance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring of handlers when contacting high-risk informants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Penalties for corrupt behaviour eg financial, professional penalties</td>
</tr>
</tbody>
</table>

### Conclusion

Currently, few studies have adequately investigated the relationship between organised crime groups and attempted corruption in the public sector. Using information from some of the few publicly available cases in Australia, it is contended that first, enhanced legislative and law enforcement responses to organised crime may lead to a tactical displacement effect, such that organised criminals may increasingly attempt to gain ‘insider knowledge’ through the corruption of public officials to reduce the risk of apprehension as they commit crimes. ICT is identified as a likely mechanism that may be embraced by organised criminals as a means to gather information on suitable targets.

The use of crime scripts analysis for understanding and preventing serious and organised crime. By exploring the extent and nature of crime displacement effects resulting from recent policy initiatives, and then analysing the crime scripts that arise in connection with the displaced criminal activity, it is possible to identify a number of opportunities for early intervention to ensure that risks of corruption are minimised. The effectiveness of using crime scripts analysis and Ekblom’s 5Is in combination has been demonstrated and should be developed and investigated further.

Although this approach has illuminated the specific process of corruption employed by criminal organisations, further evidence is required to delineate the relationship between organised crime groups and corruption in the public sector more fully. With a sound evidence base and a better understanding of the crime scripts employed (such as could be obtained through interviewing convicted offenders), situational crime prevention frameworks, such as Ekblom’s 5Is framework, could then be applied to assist in understanding the crime commission process and to reveal suitable points for effective intervention and the prevention of attempts to corrupt public officials.
References

URLs are current at August 2012


About the Authors

Elizabeth Rowe is a graduate of Queensland University of Technology and wrote this paper during an Internship at the AIC.

Tabor Akman is a Manager in the Fraud Control Section of the Audit Branch at AusAID.

Dr Russell G Smith is Principal Criminologist at the AIC.

Dr Adam M Tomison is Director and CEO at the AIC and an Adjunct Professor at the Australian Catholic University.