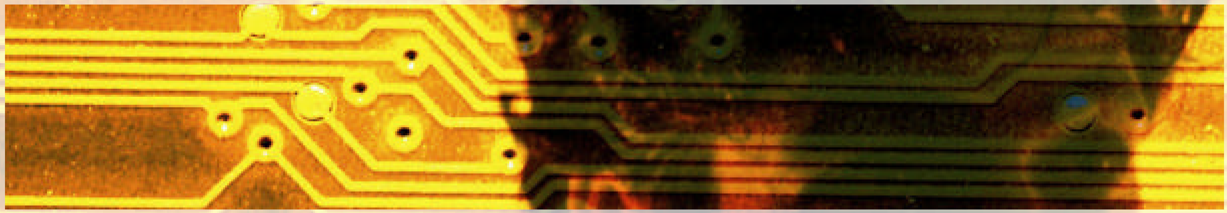
Building better partnerships with government and industry to combat cyber sabotage

Developing a safer and more secure online environment through stronger partnerships among law enforcement, government and private sectors



An AFP presentation at the *Cyber Sabotage 2002* conference held in Sydney on February27 focused attention on the development of "real partnerships" between industry and police. In this article **Jodie Durrant**, acting Coordinator High-Tech Crime, outlines how Information and communications technology has created new ways to commit old crimes and the effective investigation and prosecution of these crimes will require real partnerships between law enforcement agencies; between law enforcement and the ICT industry; and between law enforcement and the business and agencies that carry on their business in the cyber space.

If there is a simple message to be delivered to law enforcement and the private sector about cyber sabotage, e–crime and crime in general, it is that there must be better cooperation and ***real*** *partnerships – and not just stronger partnerships – between law enforcement and the private sector than there have been in the past.*

By 'partnerships' I mean the relationships between police and information and communications technology (ICT) industries as much as the relationship between police and businesses that may be the victims of crime.

While policing is often seen in the context of criminal investigations leading to prosecutions, it is always useful to reflect on the police role in crime prevention. The parameters that guide a policing organisation include recognition that:

- the basic mission for police is to prevent crime;
- the ability of police to perform their duties depends on securing the willing cooperation of the public; and
- the test of police efficiency is the absence of crime and disorder, not the visible evidence of police action in dealing with it.

These are not new concepts; the words above are based on an 1829 statement by Sir Robert Peel, the founder of modern policing.

The nature of relationships

What is a partnership? Aside from obvious dimensions of joint effort and a confluence of objectives, I will add another dimension and in so doing pick up on a comment by Elizabeth Montano, former Director of AUSTRAC and former chair of AGEC, the action group on the law enforcement implications of electronic commerce. In differentiating between cooperation and partnership, Ms Montano described partners as being people who look out for each other's interests. By that definition, while we cooperate with each other, we could not regard the police, the ICT industry and business as partners at the present time. To achieve true partnership, the "us and them" mentality must be eliminated wherever it arises.

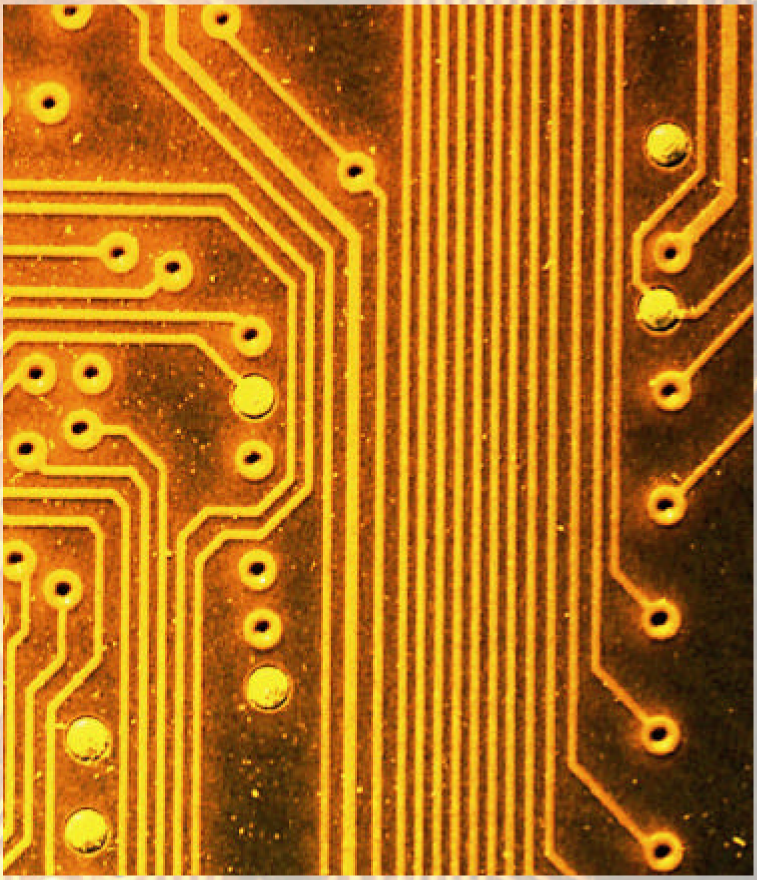
Effective investigation (and ultimately prosecution) is dependent on evidence. For example, where offences are committed by using the Internet that evidence comprises the data passing across the network and through Internet Service Providers (ISPs) between victims and offenders. If police and the ICT industry were 'partners', there would have been no need for one Internet group to establish a specialist cyber crime task force to lobby government against implementing certain overseas initiatives that regulate ISPs by forcing them to keep records and intercept transactions for law enforcement purposes.

On a similar vein, many in the community and business believe that the problems of e-crime are immense and that law enforcement is powerless to respond effectively. They believe this because some doomsayers would have them believe that law enforcement agencies are under resourced, can't retain specialist staff, are not well trained, are subject to out-of-date laws, or that police hide behind operational secrecy to restrict outsourcing.

This is not to say that issues of laws, resources, staff, training and the like are not real challenges for all law enforcement agencies but, so far as the AFP is concerned, to date those challenges have not prevented us from discharging our responsibilities to effectively deal with serious and complex crimes of this type.

This view of law enforcement failure is often subtly or otherwise reinforced. Quoting the website of one of Australia's large accounting firms (incidentally, a firm which offers fraud investigation services):

> ". . . private sector fraud services have expanded considerably in the past five years, attempting to fill the void unintentionally created by the resource restrictions of law enforcement agencies . . . investigators are shackled by resource and funding limitations and significant public and legal scrutiny, it is not so much a question of public versus private, but rather private and then public."



To repeat – police are responsible for and capable of investigating serious and complex crimes of this type.

In terms of white-collar crime generally, in the past these attitudes have led to the creation of a vast gap between the rumoured extent of the problem and that which is reported to law enforcement. As police, if we don't know about a matter, we can't investigate it. If we don't know the nature and extent of a problem, we can't gear our services to be able to deal with that problem effectively.

We also need to consider how best to serve the public interest in all of this. The website referred to above, when referring to what a victim should do about fraud (remembering that fraud is a crime) says:

> "the ability for the private sector to present a variety of alternative outcomes cannot be underestimated. These may include preparing a brief of evidence for the police to prosecute, civil recovery, insurance assessment or internal controls review, or even a negotiated outcome."

Excuse me? I don't doubt that these are all useful considerations, but surely they are not alternatives.

If criminal fraud is detected, how is the public interest served by having the private sector negotiate an outcome with a criminal rather than the proceeding with prosecution?

E-crime, cyber sabotage – the role of the AFP

The AFP is the principal law enforcement agency through which the Commonwealth Government pursues its law enforcement activities and the AFP protects Commonwealth and national interests from crime. The AFP occupies a unique position in Australian law enforcement in that its functions relate both to community policing (within the ACT and other Commonwealth Territories) and to policing of matters within the Commonwealth's interest both in Australia and overseas.

In pursuing its goals, the AFP works in partnership with the police services of Australia's states and territories, and other Australian Government agencies including those involved in law enforcement and national security.

The AFP also has extensive international links, including:

- an international liaison officer network which currently boasts 39 officers in 24 posts in 23 countries;
- providing Australia's Interpol National Central Bureau; and
- specific e-crime response mechanisms including providing a 24-hour, seven days per week contact point as part of the G8 response to dealing with hi-tech crime.

This contact point process – implemented as a result of a G8 decision – is designed to ensure a rapid and appropriate response to serious crimes in an environment where criminals are no longer restricted by national boundaries and where evidence of a crime can be rapidly lost.

In its other areas of responsibility, the AFP is also involved in law enforcement partnerships dealing with 'traditional' crimes including drug importation, serious fraud, money-laundering, exploitation of women and children; child pornography; and people smuggling – all of which may be committed or facilitated by the use of ICT, particularly the Internet. The AFP also needs to deal with new and emerging forms of crime, including such things as hacking, cracking and denial of service attacks.

If we need to have a definition, then we might want to think of e-crime as a range of illicit activities made possible by information and communications technology.

Much of what we consider to be e-crime would not be possible without networking of some form. It is the fact that computers are a part of communications network (such as the Internet) that provides the majority of opportunities for both legitimate and illegitimate activity.

One might ask whether cyber crime (including cyber sabotage) is distinct from e-crime, or a category within it? Again, to the extent that such semantics are necessary, we would clearly regard it as a subset of e-crime.

Cyber infers that it is something that occurs in the 'virtual' world of cyber space. The best representation of this in our society is of course the Internet. The same attributes that make the Internet desirable as a basis of e-commerce, also make it attractive for criminal or unlawful activity:

- the Internet represents instant global reach;
- it is quite easy to remain anonymous;
- communications or transactions can be conducted with blinding speed;
- the global connectivity of the Internet creates jurisdictional problems, and allows for the deliberate, criminal exploitation of sovereignty; and
- information and communications environments by their very nature pose evidentiary problems. Data is highly volatile, and there is generally a lack of traditional collateral (or forensic) evidence, such as eyewitnesses, DNA, or fingerprints.

The Internet itself is a vast information resource, and unfortunately, not all of the information available is correct or used for legitimate purposes. For example, would you like to be a citizen of or have a passport from the Dominion of Melchizedek? Would you like to help out a West African with some money to launder? Would you like the recipe for MDMA or perhaps an explosive? Would you like to order your drugs on line?

The majority of electronic crime that we are seeing at the moment is traditional crime – fraud, drugs, and so forth – that is being facilitated by information and communications technology (ICT). ICT has created new ways to commit old crimes.

There are also many tools freely available on the Internet that assist criminals in their activity, such as:

- anonymous re-mailers (servers on the Internet that receive and re-send traffic by replacing the original source address of the sender with the address of the anonymous re-mailer);
- packet filters or sniffers (software that allows intruders to intercept network traffic);
- nukers (software used to destroy system log trails);
- password crackers;
- scanners (software that helps with identifying

services running on networked machines that might be exploited);

- spoofers (software that allows a user to masquerade as another user); and
- automated scripts for worms and viruses, denial-of-service attacks, and Trojan programs.

All of these tools contribute to the vulnerabilities of networked computer systems, and add to the challenges facing law enforcement when dealing with technology-based crimes.

What are the major challenges for law enforcement in this environment?

From my perspective, the greatest challenge faced by law enforcement is the failure of some elements of the business community to take IT security seriously. We see many businesses engaging in e-commerce without the skills or resources to do so in a manner that might minimise the risk of crime.

No-one in their right mind would open a shop, fill it with expensive, desirable and attractive goods without investing in good locks; security systems and security personnel. No successful business critically dependent on power or communications links would operate without backup systems. No successful business would operate without financial controls, audit trails and the like.

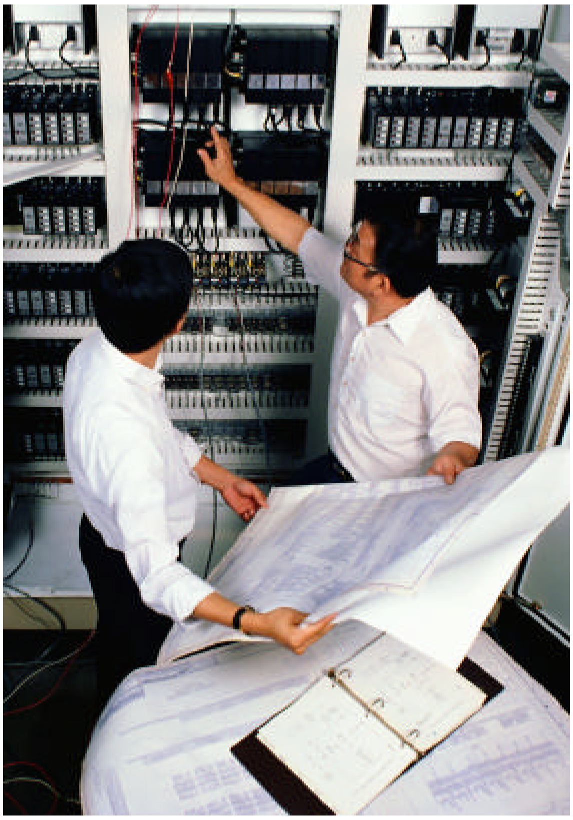
Unfortunately some businesses – and not just small businesses – don't seem to apply the same rules to their electronic businesses. I am continually amazed at some of the stupidity and naivety – and there is no nicer way of saying it – of some in business when it comes to ICT. I suspect they don't understand the technology and just don't want to know.

Many of the 'security vulnerabilities' – such as the issue with Simple Network Management Protocol (SNMP) identified recently – can be effectively addressed by simply installing software patches – but many business do not protect themselves in this basic way.

Effective IT security – and I have got to admit this is not my forte – is no different to any other form of security. You need to plan for your security. You need to identify the risks, and then having identified the risks, put in place controls to deals with those risks. Following that, those controls must be tested and audited. Security is not a product, nor is it a technology, nor is it just a cost. It must be fundamental to the business and include policy, procedures and training.

Frankly, I don't know that message is well understood or well received. A while back the AFP tried to arrange a presentation to the CEO Circle on just this subject. The presentation had to be cancelled due to lack of interest. Do CEOs realise this impacts on the bottom line? The issue is not only the cost of the crime, but damage done to reputations.

If a corporation leaves its warehouse wide open it should not be surprised if the goods are stolen – and police will investigate to the extent that is possible. Ultimately the corporation and its officers will have some embarrassment to deal with. It is no different if a website is left unlocked and credit card details are stolen. We will investigate, but it is hard to find sympathy for a business that fails to provide adequate security.



To overcome the anonymous nature of computer-related crime, the law enforcement response requires a combination of technology-based investigations and traditional investigative techniques.

Aside from working on security issues and crime prevention, there are some things that law enforcement needs to do – and is doing. To overcome the anonymous nature of computer-related crime, the law enforcement response requires a combination of technology-based investigations and traditional investigative techniques.

These investigative techniques depend on three broad strategies. Firstly, to collect direct and circumstantial evidence to prove the suspect, and only the suspect, could have perpetrated the offence. Secondly, to react quickly enough to trace the source of the criminal activity and apprehend a suspect at the source. Thirdly, to take into consideration the ongoing nature of computer-related crime and use physical and electronic surveillance to collect evidence of an ongoing or repeated offence.

However, all of this implies the availability of the same level of confidence and operability in the electronic environment that law enforcement agencies enjoy in the more 'traditional' environment. In order to achieve this operability, law enforcement needs to:

- Bridge jurisdictional boundaries

  Law makers and police remain restricted by territorial boundaries, so harmonisation of legislation and global recognition of offences is required.
- Know where to look for evidence

  Data relating to criminal business can be stored almost anywhere in the world.
- Retain and preserve admissible evidence

  Electronic evidence is volatile and thus easily destroyed.
- Deal with encryption

  Encryption is necessary for secure conduct of business and communications. Unfortunately, it is also available to criminals.
- Prove identity

  Identity is easy to forge or conceal, but is a fundamental proof needed in criminal prosecution.

Legislation needs to effectively deal with traditional crimes facilitated by technology, as well as new crimes.

- Avoid tech-lag

  Law enforcement agencies require access to cutting-edge technologies.
- Tackle the tools of crime

  The Internet and computing technology provide a ready environment for the development and distribution of tools to commit crime.
- Develop tools

  Law enforcement will need to develop or obtain its own tools and techniques for combating crime.
- Avoid disclosure of law enforcement methods

  It is not in the public interest if those tools and techniques developed by law enforcement to combat crime become widely available.
- Reduce response times where electronic evidence is involved

  As mentioned above, electronic evidence is highly volatile.
- Coordinate investigative activities

  Crimes committed using networked technologies have the potential to affect people around the world – any number of agencies may find that they have a legitimate interest in investigating the activity.
- Develop strategic partnerships and alliances

  Law enforcement will have to forge partnerships with those for whom the maintenance of technological expertise is core business.
- Provide training at all levels

  Law enforcement will have to maintain a current knowledge and understanding of technologies to be able to make sense of high-tech crime.
- Retain and develop specialist staff

  Even with training of staff at all levels, specialist staff will always be necessary in the high-tech environment.
- Contribute to government processes for law reform

  Legislation needs to effectively deal with traditional crimes facilitated by technology, as well as new crimes. Law enforcement powers need to be effective in the high-tech environment. In that respect, we obviously welcome the *Cybercrime Act 2001* which provides law enforcement with essential tools to investigate in cases where criminals use technology, like computers, to carry out or to facilitate their unlawful activities.

Advances in computer technology and electronic communications have created new means and possibilities for committing cyber crimes such as hacking, denial of service attacks, and virus propagation. The new computer offences in the Cybercrime Act are designed to address these forms of cyber crime, as well as conduct that impairs the security, integrity and reliability of computer data and electronic communications. The Act also enhances the operation of existing search-and-seizure provisions relating to electronically stored data, by amending the *Crimes Act 1914* and the *Customs Act 1901*.

This is a very large menu. Law enforcement agencies are not going to be able to achieve these things in isolation. Quite simply, law enforcement needs partners – "people looking out for our interests" as Elizabeth Montano puts it – if we are to remain effective in the current and emerging environments.

The AFP is involved in many cross-agency, cross-jurisdictional fora that are examining electronic crime and wider issues, such as the Police Commissioners' Conference E-Crime Project, the Action Group into the law enforcement implications of Electronic Commerce, and the Commonwealth's E-Security National Agenda. All of these fora include a focus on developing partnerships and pursuing cooperation with both private and public sector entities.

The Police Commissioners' Conference E-Crime Project

The Police Commissioner's Conference involves the Commissioners of all Australian states and territories, as well as New Zealand, Fiji, Papua New Guinea, and of course the AFP.

In March 2000, the Police Commissioners held a conference, the theme of which was *Crime at the speed of thought*. At the conference, the Commissioners decided to place the issue of electronic crime on the law enforcement agenda. The PCC e-crime project included the exploration of the problem, through a detailed and comprehensive scoping paper, and the subsequent development of an electronic crime strategy supported by a work plan.

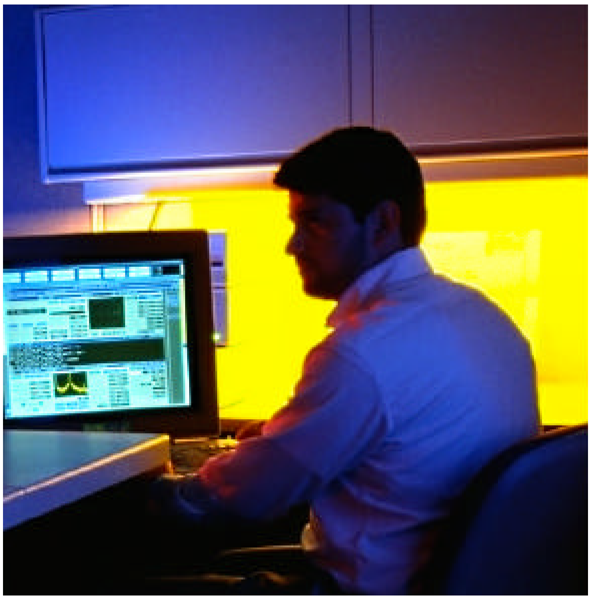
The strategy purpose is "to provide a safer and more secure community by preventing and reducing electronic crime". The strategy focus areas are:

- prevention;
- partnerships;
- education and capability;
- resources and capacity; and
- regulation and legislation.

Of most import to this conference is the focus area of 'partnerships'. Pursuit of this objective will be through three complementary objectives, which are to:.

- establish and maintain effective working relationships with international law enforcement, government, and private agencies;
- promote private sector leadership, including self regulation wherever possible, and practical regulation where necessary; and
- develop and maintain partnerships with communities, interest groups and non-government organisations.

The main agency tasked with facilitating these objectives is the Australasian Centre for Policing Research, in its capacity as Secretariat for the PCC. Since the endorsement of the strategy mid-last year, the ACPR has been engaged in foundation work on these objectives, through examination of existing stakeholder interests and roles, and existing formal and informal relationships relating to e-crime between law enforcement and other bodies.



Law enforcement powers need to be effective in the high-tech environment.

A second multi-agency forum that the AFP has been involved in since its inception is the Action Group into the law enforcement implications of Electronic Commerce (AGEC)

The AGEC (formerly 'Research' Group) was formed in 1997 as a response to the Heads of Commonwealth Operational Law Enforcement Agencies' (HOCOLEA) need to research the impact of electronic commerce on law enforcement and revenue agencies' ability to provide a safe community.

AGEC is currently chaired by the Director, AUSTRAC and membership includes AFP, NCA, ATO, ACS, CDPP, ASIC, ACCC, DIMIA and ACPR.

AGEC's action plan sets out its objectives and supporting activity. The objectives that are relevant to this article are to work with business and industry to raise awareness and adopt e-commerce risk-management strategies; and encourage the development of formal IT skills development and security training.

The AFP has been a significant contributor to many of the AGEC initiatives, most of which have involved the development of papers addressing specific issues relevant to e-commerce and law enforcement. These issues papers are released publicly and help inform government and the public and private sectors of emerging information and communications technology issues that law enforcement and regulatory agencies see as impacting on our community.

The AFP is also part of two important AGEC sub-groups, and these are the legal update group and the Cybercrime Task Force:

- Legal Update Group

  The Legal Update Group (LEGUP) most recently has been considering issues such as: record keeping requirements for the Internet industry; identity theft; an offence of 'wire fraud'; and law enforcement access to open vs unopened e-mail.
- Internet Industry Association Cybercrime Task Force

  A small sub-group representing AGEC is currently engaged in negotiations with the Cybercrime Task Force established under the auspices of the Internet Industry Association (IIA). The aim of this sub-group is to negotiate with the IIA an industry code for Internet service providers, to clarify the Internet industry's obligations and relationship with law enforcement agencies, especially with regard to the investigation of criminal activity.

The third major forum that is probably most relevant in light of recent events, and that is the:

- Commonwealth e-security national agenda

  Efforts in regard to the e-security national agenda are directed at achieving the strategic goal of creating a secure and trusted electronic operating environment. You may note this objective is not that dissimilar to that of the E-Crime Strategy.

Effective investigation and prosecution will require true partnerships between law enforcement agencies; between law enforcement and the ICT industry; and between law enforcement and the business and agencies which carry on their business in the electronic medium.

A major component of this agenda is realising coordinated arrangements for protection of the National Information Infrastructure (NII). The key functional groupings of the NII are telecommunications, banking and finance, transport and distribution, energy and utilities, information services, and other services including defence and emergency. Australia's economy is highly dependent on the efficient functioning of its NII, and many agencies are working together to realise this strategic goal. The lead agency for facilitating the Commonwealth's e-security national agenda is the National Office for the Information Economy (NOIE).

Again, an important component of this agenda is achieving stronger relationships with the owners of the NII through awareness raising and information sharing. A broad-brush description of NOIE's objectives is:

- information sharing arrangements with industry and government;
- incident reporting–initially Commonwealth, with a view to extending arrangements to state/territories and possibly specific private sector;
- skills development – with a view to increase the number of skilled IT Security personnel;
- awareness raising – across owners of critical infrastructure components, other organisations, and vulnerable groups in our community.

Up skilling for the emerging environment

We may find that sometime in the future we don't need to use terms like 'electronic crime' or 'cyber crime', instead choosing to focus more on what was done as opposed to how it was done. We may even find that technology will become as invisible to us as motor cars are today. But until those days arrive – when law enforcement officers can drive computers as well as they can drive cars – it will be necessary for law enforcement agencies to have a special focus on "electronic crime".

All law enforcement agencies are going to have to continue the process of up-skilling their personnel to equip them to deal with the emerging environment.

But it is not a matter for law enforcement alone, or even primarily for law enforcement. The wider community needs to take IT security more seriously and develop appropriate skills within the community and industry to better protect itself. And when the inevitable crime occurs, it must be reported.

Effective investigation and prosecution will require true partnerships between law enforcement agencies; between law enforcement and the ICT industry; and between law enforcement and the business and agencies which carry on their business in the electronic medium.

When we are all looking out for each other's interests, then – and only then – will we be able to say that we are truly well equipped to deal with these types of crimes. Perhaps then, we may truly see an absence of crime and disorder.