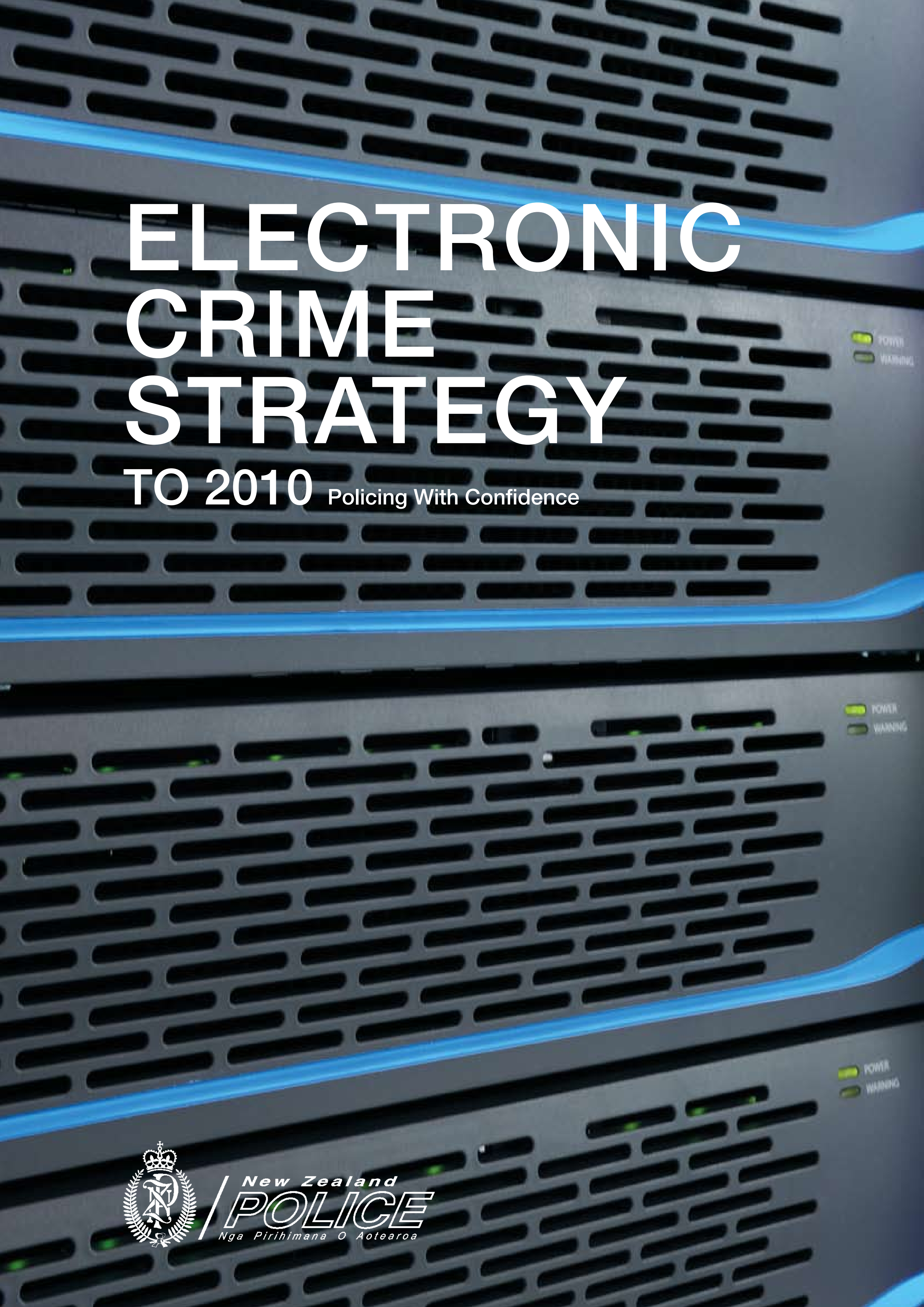


ELECTRONIC CRIME STRATEGY

TO 2010 Policing With Confidence

New Zealand
POLICE
Nga Pirihimana O Aotearoa

Commissioner's Foreword

New communication and computer based technologies offer benefits to New Zealand communities. They also present opportunities for criminals to commit crimes in new ways and provide opportunities to inflict harm and cause loss. The increasing uptake of technology by criminals means some types of crime can now be committed faster, against more victims, with anonymity and for greater gain. Crimes now occurring in the electronic environment include traditional offending, such as fraud and paedophilia, and emerging new crimes such as denial of service attacks and hacking. Of great concern is organised criminal use of information and communications technology to conceal their activities, reach a wide range of victims, and network with other criminal groups.

Through this strategy, we will ensure that Police are positioned to address the use of technology by criminals and can respond to new types of electronic crime (e-crime).

Since 2001, we have been collaborating with Australian Federal and State Police in our response to e-crime. These arrangements have worked well and we will continue to work closely with the new high-technology crime centre those agencies have established. However, over the past five years there have also been developments in New Zealand, which now make it appropriate for the New Zealand Police to articulate its own strategy.

In recent years we have bolstered the size of our e-crime laboratory, responding to increasing demands for electronic forensic input into criminal investigations, and we have started to train staff about how to deal with electronic evidence. Among our partner agencies, a centre for critical infrastructure protection (CCIP) has been established to address threats to critical infrastructure and Government's digital strategies have led to a variety of other initiatives to enhance electronic security and address e-crime.

This strategy places a great deal of focus on a combined agency response to e-crime. Police are only one interested party among Government, industry groups and others playing a role in the security and safety of the electronic environment. As well as endorsing collaborative approaches, this strategy will lead to further development and maintenance of our own internal capability.

These strategies will ensure that crime reduction capabilities are maintained and complement the efforts of other organisations involved in keeping New Zealand's electronic systems and their users safe and secure.

Howard Broad
New Zealand Police Commissioner

Contents

Much e-crime is unsophisticated. It often involves activities on the Internet such as trading stolen property through auction sites, obtaining stolen credit card information from newsgroups and chat rooms, distributing pirated intellectual property, and dealing drugs through email and websites.

The Internet has provided considerable opportunity for many offenders to extend their supply and customer networks and exploit the reach of the medium – just as it has provided the same advantages to legitimate users. The use of technology for these criminal purposes causes challenges for Police because of sometimes demanding investigative requirements and apparent significant growth in some crime.

Electronic Crime

Definition

Police agencies worldwide have struggled to define their role in policing e-crime and to understand how to be effective in addressing the problem. This is partly because these types of crimes are extremely diverse. New Zealand Police consider electronic crime (e-crime) to cover:

All offences where information and communications technology is:

1. **used as a tool in the commission of an offence**
2. **the target of an offence**
3. **a storage device in the commission of an offence.**

E-crime includes traditional offending facilitated by technology such as telephony, the Internet and encryption. It also involves computer attacks. However, it is important to recognise that the bulk of e-crime we currently see is not attributed to hackers. In New Zealand, e-crime mostly involves traditional offending with components having electronic means. This includes trading in illegal drugs, fraud, harassment, and many other types of criminal activity. Information technology has particularly influenced some traditional offending. Most notably, this includes:

- fraud
- identity theft
- organised crime
- paedophilia

However, e-crime also includes new activity such as attacks on computers and new opportunities for crime enabled by electronic systems, such as services theft and software piracy. Worldwide these are significant and new problems.

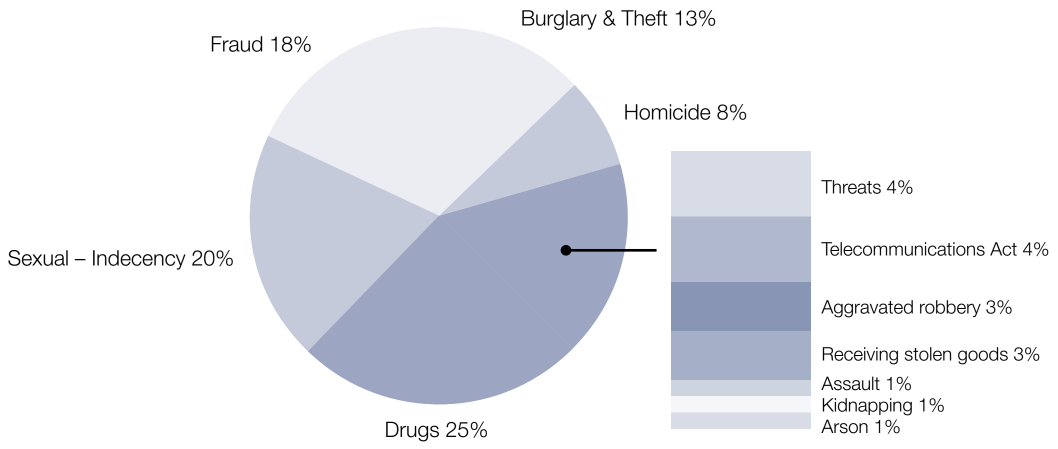
Nature of Electronic Crime Problem

Criminals have exploited developments in information and communications technologies. It has provided them with new tools and facilitated new criminal activity, which can now target computing infrastructure. Criminals can also exploit the fact that offending can easily cross jurisdictional boundaries and large distances. Increasing bandwidth, as well as supporting growth in commerce, is also increasing opportunities for criminals. Potential victims are becoming increasingly available as more people use these technologies. Many of these new users represent easy targets because they lack online security awareness or skills.

Measuring e-crime problems affecting New Zealand is hampered by a lack of data for offences involving electronic components. The recent successful transfer of Police operational computer systems to NIA (the National Intelligence Application) and a Police Crime Statistics Strategy provide an opportunity to improve e-crime recording. This should allow for the capture of e-crime connections to relevant offences.

Local and Australian victimisation studies have collected some information about e-crime prevalence, though mainly about computer attacks. Most studies have not quantified growth in traditional crime facilitated by electronic means. However, Police have monitored the demand for forensic analysis of e-crime exhibits by the Electronic Crime Laboratory (ECL). The number of crimes involving electronic evidence has increased ten-fold over the past eight years. Electronic evidence is increasingly prominent in some types of offending such as fraud and sexual crime.

Proportion of Electronic Exhibits Processed by ECL



Identity crime is one of the fastest growing types of crime in the world, and is defined as any offence involving the misuse of a personal identity. The majority of identity crime is committed with the help of computers.

Identity crime often involves criminals obtaining information from everyday transactions like:

- bank and credit card numbers
- names
- addresses
- driver's license details
- log-on details for other services

Criminals then use this information to commit fraud and theft. Opportunities in this area are increasing with the development of online auctions, gaming and other services.

Computer users and businesses need to be vigilant to ensure that personal information is managed cautiously and with heightened security. This applies to the security of online transactions, paper waste containing sensitive information, personal details in wallets and purses and information on portable computers.

Identity crime is a growing global problem – it knows no boundaries; victims and criminals can be on opposite sides of the world making it difficult for local law enforcement agencies to investigate the crime, catch the perpetrator, or help the victim.

The involvement of organised criminals in e-crime is a concern to Police.

Organised criminals exploit sovereign states that support illegitimate Internet connections. These locations offer safe havens from external authorities and have limited restrictions on activities such as trading pornography, money laundering, pyramid selling, and other activities that would be illegal in many other jurisdictions.

The threat of organised crime is real. Unfortunately it is very difficult to assess the size and impact of organised crime groups. This is because by its very nature organised criminal offending is usually hidden.

The increase in organised criminals' use of secure communications technology, the potential for global reach and the connection of organised criminal networks internationally, are significant concerns to Police. Also worrying is the growth in opportunities for organised criminal exploitation of electronic commerce and the new vehicles that are available for laundering money and goods that are facilitated by the Internet.

Other jurisdictions already report significant organised crime involvement in the Internet and the use of other technologies (such as secure mobile telephony) by these groups. Particular evidence exists for the involvement of organised crime in credit card fraud, money laundering and identify theft.

Policing Challenges

The attributes of e-crime pose challenges. These include anonymity, global reach, the speed by which crime can be committed against multiple victims, the potential for deliberate exploitation of sovereignty issues, and the volatility of evidence. These features create obstacles to detecting and tracking criminals. Techniques used by criminals range from false Internet accounts to the use of secure Internet and telephone communications. A particular risk is that the now widespread availability of encryption enables criminals to communicate with each other with minimal risk of discovery.

Responding to these challenges requires expertise and resources beyond the current capability of mainstream Police. Perhaps the biggest problem is the pressure to keep pace with increasing technological sophistication. This includes maintaining the skills and resources required to provide advice on crime prevention, and the skills required to respond, investigate and prosecute offenders. The availability of these skilled resources within Police is limited. Most critically, we face a capability gap among generalist staff. With many traditional crimes now involving electronic devices, any lack of knowledge and skills has the potential to compromise investigative outcomes. Importantly though, investigating e-crime still requires many traditional policing methods that remain a strength of Police in New Zealand.

As a result of the growth in e-crime our specialist forensic capabilities are continually stretched. There is an ongoing demand to grow forensic capabilities to keep pace with the increasing requirements for electronic evidence and to provide investigators with assistance required on other technical aspects of e-crime investigations.

In addition to limited resources, Police face problems with a legislative framework largely based on physical world constructs. The current regulatory environment sometimes limits access to evidence, because of the dependence of Police on external organisations, such as Internet service providers, to enable access to information about criminal activity. Criminals also exploit the inter-jurisdictional difficulties in pursuing investigations.

A public perception that Police or other government agencies are not equipped to respond to e-crime may result in the feeling that there is little benefit in reporting incidents. In the case of threats to electronic commerce or other business activities, the concerns of business are often continuity and reputation related. Business can be motivated not to report crime because publicity will harm business.

E-Crime Strategy

The e-crime strategy outlines the Police approach to combat e-crime over the next five years. The strategy aims to better position Police to deal with e-crime moving forward – the first steps toward establishing a much larger core of specialist forensic and investigative expertise.

New e-crime prevention and problem-solving approaches are required to protect potential victims and environments. To facilitate these approaches it is necessary to align intelligence systems, tools, investigative requirements and laws to address e-crime issues.

This strategy provides a framework for future planning and will give certainty to partner organisations about the directions being followed to prevent and respond to e-crime.

Strategic Alignment

The strategy demonstrates commitment to Police's high-level outcomes of confident, safe and secure communities, less actual crime and road trauma, fewer victims, and a world class Police service.

Outcomes

The desired outcomes include:

- a safe online environment by reducing e-crime offending and minimising the harm caused to people and organisations in New Zealand, and
- improved e-crime investigative and forensic capability leading to increased crime resolution

Principles

The following principles guide this e-crime strategy:

- Police will adopt a collaborative approach using multi-agency methods and networks.
- Police will not duplicate services or capabilities offered by other agencies.
- Police will adopt knowledge and intelligence-based approaches to the deployment of preventive and detective activities and resources.
- Police will engage internationally to monitor and respond to emerging risks and opportunities.

The Government is targeting information and computing technology growth and innovation to "grow an inclusive, innovative economy for the benefit of all". Achieving this goal depends on growing New Zealanders' confidence in using new technologies safely. A safe and secure digital environment is essential to the success of the Government's digital strategies.

One strategy is e-government. This has been developed as a vision to enable all New Zealanders to access government information and services using the Internet, telephones and other technologies.

The e-government unit is focused on building electronic security through initiatives such as online authentication to provide a means for people and government agencies to verify their authenticity when making electronic transactions.

Police Strategic Plan to 2010, Strategic Goals:

Community Reassurance:

- provide opportunity for participation
- set local priorities
- work in partnership
- provide protection

Policing with Confidence:

- evidence based proactive policing
- timely and effective response to calls for service
- thorough investigations
- effective resolutions

Organisational Development:

- leadership and people in policing
- integrity and accountability
- technology and innovation

Goals and Objectives

Police will actively support government goals and initiatives enabling information, communications, and technology (ICT) in New Zealand and furthering international commitments to enhance New Zealand's cyber security and cyber crime defences.

Police will build the capability and credibility to effectively investigate and resolve e-crime.

Police will target the following objectives in keeping with overall strategic goals of community reassurance, policing with confidence, and organisational development.

Key initiatives of Partnerships, Organisation, Capability, and Integrity contribute to achieving the objectives.

Community Reassurance		Partnerships	Form significant e-crime prevention and detection partnerships through collaboration with other Government, international, and industry groups.		Partnerships
	Policing With Confidence	Responsiveness	Respond to offending by investing in capability to effectively detect and apprehend criminals where electronic media is used for, or associated with, the commission of crime.	Organisation	
Organisational Development		Intelligence	Adopt an intelligence-based approach to analysing e-crime problems, producing quality information to support the deployment of resources.		
		Investigations	Improve front-line investigative capability, response, and understanding of e-crime through enhanced skills and tools.	Integrity	Capability
		Forensics	Meet increasing forensic specialist and inter-jurisdictional demands, by focussing the ECL with the capacity, tools and skills to meet international laboratory standards.		

Organisation

Police will demonstrate their commitment and understanding of the significance and priority surrounding e-crime by establishing the National Cyber Crime Centre (NC3) and aligning the Electronic Crime Laboratories (ECL) under a single national structure.

A nationally focussed unit will improve Police's coordination with Government and key industry groups within New Zealand and other international groups and jurisdictions – both at strategic and operational levels.

National Cyber Crime Centre (NC3)

The National Cyber Crime Centre (NC3) is a specialist e-crime response and investigation group that will:

- provide a single reporting point for e-crime able to be accessed through traditional telephone reporting channels and through enhanced Internet contact points, enabling the collection and investigation of complaints
- coordinate Police's response to e-crime reported in New Zealand
- coordinate Police's response to trans-national e-crime – in which there can be any combination of New Zealand or overseas victims, offenders, and technologies involved in the commission of an offence
- proactively target and electronically patrol places where crime occurs, focusing on high priority areas such as organised crime, violence, and online child exploitation

The NC3 will be a national facility with a central base and core team of dedicated specialists located in Wellington, working closely with the specialist capability already existing within the ECL. The central Wellington location aligns with key partner organisational structures and response units eg Centre for Critical Infrastructure Protection (CCIP), Interpol, Customs, and the Department of Internal Affairs (DIA).

The NC3 will complement traditional investigations, assisting initial high-level e-crime investigations to determine criminal activity, and providing specialist assistance where criminal activities enter the electronic world.

The principles and protocols surrounding how the NC3 will operate need to be identified and agreed, and this will be cognisant of similar centres established by other jurisdictions (and their lessons learnt), and any wider sector initiatives that might arise to establish a New Zealand based computer emergency response team (NZCERT).

Appendix A contains a high-level diagram of the e-crime structure.

Australasian Police agencies have established the Australian High Technology Crime Centre (AHTCC). Its role is to provide a nationally coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes (especially those beyond the capability of single jurisdictions); to assist in improving the capacity of all jurisdictions to deal with high tech crime; and to support efforts to protect the National Information Infrastructure.

The United Kingdom set up a national high-technology crime unit in the year 2000, following recommendations of a computer crime working group of the Association of Police Officers. The unit has since been transferred into the Serious Organised Crime Agency. The unit provides e-crime investigative capability and maintains a national capability to address e-crime threats. The unit also supports investigations, intelligence, technical support, and forensic retrieval of digital evidence.

The Royal Canadian Mounted Police have formed a distributed network of computer crime response units under the banner of a Technological Crime Program. The group research and develop computer forensic tools and provide forensic assistance to domestic and international accredited agencies and Police services.

The ECL evolved in the early to mid 1990s, and subsequently from the necessity for Police investigators to have computer forensic skills in Districts.

The Police Executive approved the current ECL structure in October 2000, and the ECL now operates with a staff of 18, over three locations.

Establishment of the ECL was in line with best practice models under development by the Australian Centre for Police Research (ACPR). Structured, high-level coordination at a national and Australasian level, and the development of police capability and capacity were two of the guiding principles contained in the Electronic Crime Strategy of the Police Commissioners Conference in March 2001.

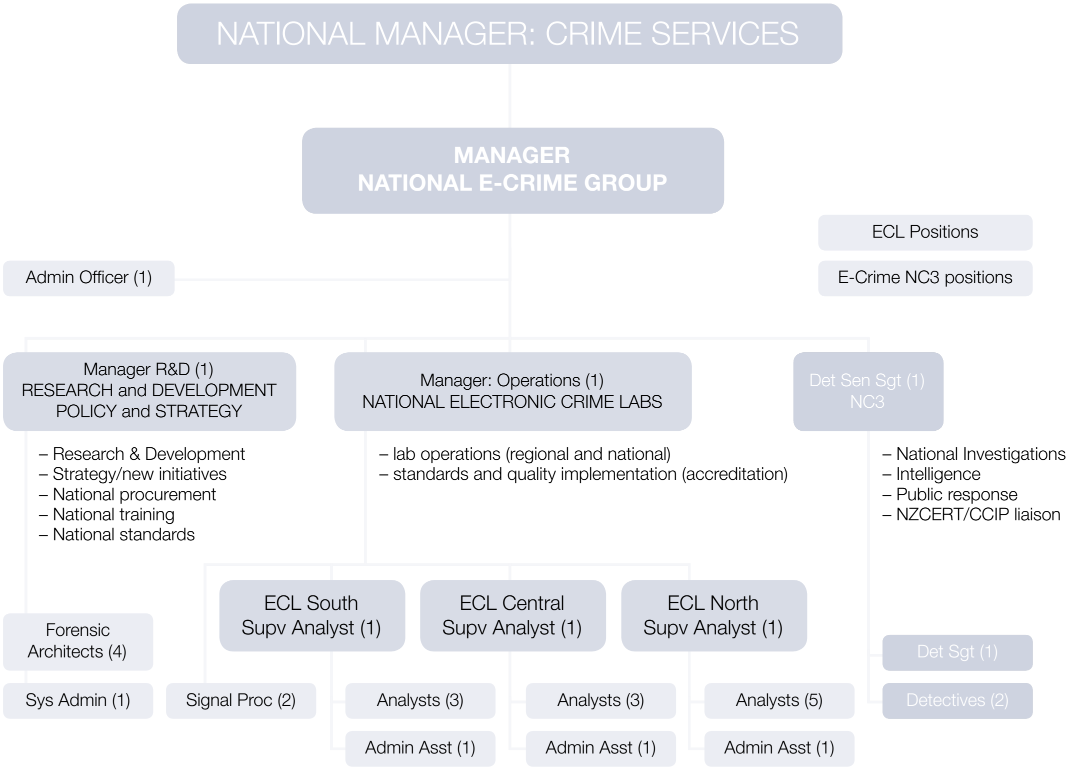
The ECL was intended to provide the New Zealand Police with a formalised, national forensic computing capability.

ECL and E-Crime Structure

A review of the ECL recommended ways to address issues with the ECL staff turnover rates, training and career structures, and workloads. Several of the recommendations made have already been implemented. Those remaining include moving to a revised national structure, which is incorporated into a proposed overall e-crime structure as shown below.

The drivers for restructuring the ECL include:

- raising the profile of the ECL to reflect national rather than District based response (ECL will continue to work with their local Districts for established local priorities)
- increasing the focus on strategy and development of key partnerships
- maximise the time ECL specialists spend on specialist forensic work, by providing operational management and administrative support roles
- prepare the ECL for international accreditation (see Integrity section, page 16) which requires a single 'authority' responsible for assigning responsibilities, accountability, unity of command, and performance
- alignment of the ECL with the proposed NC3
- simplified reporting and line management
- improved consistency of processes across ECL locations



Partnerships

Police cannot effectively address e-crime issues alone. This is because of its size, complexity, the technical resources required to respond, and the limited amount of reporting to Police that occurs. These factors mean Police are dependent on other organisations. The challenge is to enhance cross-agency and public-private sector cooperative approaches. This includes combining complementary specialist expertise, intelligence and other resources.

Police continue to encourage organisations that enhance security of the electronic environment. The wider government sector is already showing leadership on these issues through its digital strategy and e-Government initiatives. Police will continue to contribute enforcement perspectives to these initiatives.

From Police's perspective, the objectives of these partnerships is to promote security policies, private sector leadership (including self-regulation), and government regulation where required. Police wish to ensure that significant crimes are prevented and that the electronic environment retains the community's trust and confidence.

Government

The Centre for Critical Infrastructure Protection (CCIP) is the main government agency focused on protecting public and private organisations that supply services such as power, telecommunications and health care from computer misuse and hacking. Police will coordinate with the CCIP in responding to e-crime incidents affecting critical services, formalising requirements to collect evidence and meet other criminal investigative obligations.

The other operational agencies involved with Police in responding to reports of e-crime are the Customs Service, Security and Defence agencies, and the Department of Internal Affairs. Police will continue relationships with these agencies, building protocols for effective coordination through mechanisms such as Combined Law Agency Groups, the Departmental Committee on Computer Security (which sets and reviews national computer security policies) and the Officials' Committee for Domestic and External Security.

The Information Technology and Telecommunications Policy Group in the Ministry of Economic Development, the ICT branch in the State Services Commission, and CCIP all initiate activities that require Police support. Police will support and contribute law enforcement perspectives to these initiatives.

In the case of business or government infrastructure, it is important that any systems compromised in a computer attack are restored as quickly as possible.

Owners of New Zealand's critical infrastructure are provided with government support to protect and restore critical services. The Centre for Critical Infrastructure Protection (CCIP) provides this support.

New Zealand Police work closely with the CCIP to ensure that alongside any need to re-establish critical services, requirements for evidence are fulfilled in the event that this may be required in a criminal investigation.

The CCIP is a unit of the Government Communications Security Bureau. It has a web site at www.ccip.govt.nz

The ICT group of the State Services Commission (SSC) has proposed a Computer Emergency Response Team (CERT) in response to various international commitments under OECD, APEC and the ASEAN Regional Forum, aimed at promoting trust and confidence in information technologies in New Zealand. A CERT closely aligns with the CCIP functions, but provides cover beyond critical infrastructure, for key societal and commercial sectors as well as the public.

The Crimes Amendment Act 2003 came into effect on 1 October 2003 and created four distinct new computer crimes.

1. Accessing a computer system for a dishonest purpose.
2. Damaging or interfering with a computer system.
3. Making, selling, distributing or possessing software for committing crimes.
4. Accessing a computer system without authorisation.

This legislation now gives strong new protection against hackers.

The Telecommunications (Interception Capability) Act 2004 came into force on 5 April 2004. That Act allows Police to effectively carry out the lawful interception of telecommunications under an interception warrant obtained in circumstances such as where there are grounds for believing there is an organised criminal enterprise, serious violent offence, or drug dealing offence.

A network operator must ensure that they provide an interception capability (although there is up to a five-year lead-in time for existing network operators to provide the necessary interception capability). This law brings New Zealand into line with other countries that allow their law enforcement agencies similar access.

Industry

The Security Research Group (SRG) of the University of Otago in partnership with the Computer Security Institute (CSI), the CCIP and Police, produced the 2005 New Zealand Computer Crime and Security Survey of New Zealand businesses. The 2005 survey found 60% of respondent organisations had experienced electronic attacks originating outside the organisation, showing a steady growth over the past five years. Average annual losses were estimated at $43,000 per organisation.

Prevention of e-crime relies on industry organisations and public awareness. Having an effective regulatory environment helps to ensure that organisations take measures to protect consumers. Police will support groups such as the Internet Safety Group, who assist in heightening community awareness and provide policy responses to e-crime issues.

Specialist ICT sector input is required for an effective response to many types of e-crime. Police will work with Internet service and telecommunication providers to enable access to records of traffic information to assist the investigation of crime (pursuant to search warrants).

It is essential to keep abreast of technology trends and changes in commonly used technology. Police will continue to establish and maintain relationships with major technology stakeholders, eg Microsoft and Cisco.

International

International partners include the G8 sub-group on High Tech Crime, Interpol, and the US Federal Bureau of Investigation. The South Pacific Chiefs of Police forum and the Australasian Police Ministers Council (APMC) are forums to coordinate regional response capability. Police will work with the APMC to improve the regular sharing of information, skills and response capability among e-crime managers.

Inter-jurisdictional responses to e-crime are reliant on solid relationships and cooperation with international law enforcement organisations. Police will work with the United Nations Convention against Trans-National Organised Crime to address issues hindering Police ability to deal with international jurisdictions, including provision of mutual legal assistance, extradition, law-enforcement cooperation and technical assistance.

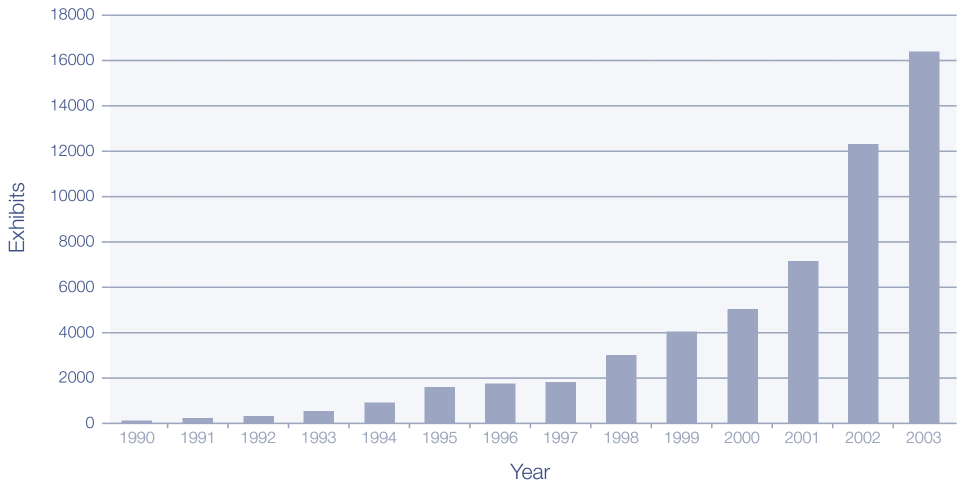
Capability

Enhancing the skills to gather and assess electronic evidence is required to deal with information and communication technology issues that now confront many investigations. Equipping detectives and other staff with the skills to recognise and deal with electronic evidence will ensure that skills are available to conduct most Police investigations.

Police maintain the ECL to provide forensic support to investigations and prosecutions. These serve Police and other law enforcement agencies. The ECL currently comprises 18 staff located in Auckland, Wellington and Dunedin. Their capabilities include signal processing, computer examination, forensic software development, and the search and seizure of electronic evidence. The group also maintains partnerships with computer crime agencies and links to Internet and telecommunications providers.

For the past five years, the ECL has experienced significant growth in demand. During 2003, requests were received for the analysis of 16,300 items of forensic evidence.[1] This demand outstrips the ability of the laboratory to service the majority of investigations involving electronic evidence.

Number of Exhibits Presented to ECL



Essentially, the identification and recovery of electronic evidence can be grouped into three levels of complexity:

Level 1: Identification of directly visible evidence

Level 2: More intensive searching of contents and recovery of data (eg deleted files) to identify less obvious or latent evidence using specialist equipment and tools

Level 3: External specialist expertise required, eg from hardware vendors.

The availability of computer evidence is increasingly providing Police investigations with powerful evidence.

Criminals use computer devices for record keeping, as communication tools to plan crimes, as devices to execute fraud, to transmit pirated software, and a host of other illegal activities. In some cases, computers may simply serve as a silent "witness" to a crime by storing information relating to the offending.

A criminal's computer often contains incriminating evidence that might never have been accessible 20 years ago. For example, criminals using the Internet leave behind a trail of evidence that Police and other law enforcement agencies can use to identify them and their offending.

[1] Comparable statistics indicating the investigative demand for recovering e-crime exhibits are not available from 2004 onwards. This is because submission processes were changed during 2004 to relieve pressure on the ECL by restricting submissions to high priority exhibits, as determined by District Crime Managers.

Dunedin-based ECL staff have been operating preview clinics for one week of each month, in Christchurch.

The clinic provides an opportunity to preview seized electronic equipment and identify any obvious evidence.

Many of the cases previewed at the clinic might otherwise not have been submitted to the ECL.

In one clinic alone, of the 36 items previewed:

- 5 contained evidence of child abuse or objectionable material
- 10 provided leads to aid in associated investigations
- 3 contained evidence of money laundering or fraud
- 8 items identified suspects in receiving or burglary cases
- 1 contained evidence relating to a drugs investigation
- 1 was submitted for further specialist analysis and recovery at the ECL

When the ECL was first established, specialist skills and equipment were needed to perform Level 1 analysis, requiring that all jobs relating to electronic evidence be submitted to the ECL for full analysis and evidence recovery.

Technology has since moved on, and more tools are now available, making it easier for non-specialist staff to perform Level 1 analysis (with assistance from the ECL). This development has yet to be reflected in the workload of the ECLs with most jobs still submitted for full analysis.

The proposed development of additional tools will simplify some Level 2 analysis enabling more identification of evidence by staff outside the ECL, and reduction in the overall ECL workload.

Improving Frontline Capability

The high ECL workload is resulting in delays in processing electronic items, which can compromise investigative outcomes. Moving Level 1 activities from the specialist ECL to frontline staff (supported by the ECL) will enable a faster turnaround time and reduce the ECL workload.

Preview clinics take the ECL specialist capability out to each District on a regular basis, with ECL staff working alongside investigators to securely (without endangering the exhibit or potential evidence) view the contents of seized computers or disks and identify items of interest. Such Level 1 type analysis will often identify all that is needed for the investigation, although subsequent Level 2 type analysis can be initiated if required. This approach enables a focussed investigation of disk contents, and avoids specialist effort on misdirected analysis and unneccessary reporting.

Preview clinics are already held each month in Christchurch, and although the number of items previewed each month may vary, there is a consistently high success rate (refer sidebar).

Police will extend the use of preview clinics to each District.

Recovery of evidence from mobile phones is another growth area for the ECL. The extraction of photos or other information contained on a mobile phone in an evidentially safe manner requires some specialist tools that can be made available to frontline staff.

Mobile phone booths have already been established in some Districts enabling local staff to obtain information (eg, photos, messages, contacts, or complete SIM dump) directly from seized mobile phones, without intervention from ECL staff.

Police will implement mobile phone booths in each District with appropriate support and guidance for District staff.

District Liaison

Improved communications to frontline staff will aid their understanding of e-crime, electronic evidence, and the services available through the ECL. Introduction of the above initiatives will also require assistance from Districts to provide local liaison points, contacts for scheduling preview sessions, and to generally act as a local champion for the ECL.

E-Crime Liaison Officers are proposed for each District – either as a dedicated staff member or in conjunction with other duties (depending on each District's size and requirements).

Police will appoint E-Crime Liaison Officers for each District to facilitate local ECL activities and communications.

Research

Police wish to build an accurate picture of e-crime offending and continue to encourage all victims to report offences. We need this picture because crime reduction relies on understanding the criminal environment as a critical first step in effective problem solving. The intelligence picture will be used to influence public and private sector organisations and individuals who can impact on electronic security.

Police will encourage the sponsorship of research to clarify the extent, scope, and impact of e-crime in the New Zealand setting.

Police will collect and analyse e-crime data, providing intelligence and direction to investigations, and strategies to address e-crime.

An E-Crime Liaison Officer in each District can:

- liaise with the ECL over case submissions and priorities
- assist investigators in using provided tools to identify evidence
- assist ECL staff in scheduling preview clinics and sessions
- prepare exhibits for preview sessions
- provide guidance for District staff in seizing electronic exhibits
- provide onsite support for mobile phone booths, assisting staff and maintaining equipment
- coordinate the introduction of ECL initiatives (eg Project EVE)

Currently any evidence obtained from the examination of electronic equipment by ECL staff is stored on individual hard drives that are held within caddies and need to be loaded manually for each case to be examined.

With EVE, when a computer is seized and provided to the ECL, staff will create a virtual 'image' from the physical computer then run specialist analysis and indexing tools to enable the search capability. The virtual copy is then placed on a Storage Area Network (SAN) and made available to the frontline investigator via the Police enterprise network.

When an investigator accesses the virtual copy it is loaded as a virtual machine and they can then see the computer in the same way the suspect sees it. Using simple search tools the investigator can quickly search through the data on the computer to identify anything relevant to the investigation.

The introduction of EVE is expected to reduce lead times in obtaining electronic evidence from months down to days, significantly increasing the throughput of the ECL and the investigative capability of the investigators.

Environment for Virtualised Evidence (EVE)

Current inability to process the high volume of electronic exhibits seized during police investigations has prompted the need to develop a more effective system to conduct these types of specialist investigations.

Project EVE involves the development of a virtual forensic evidence recovery environment that will move the ability for general investigative interrogation to front line investigators via specifically targeted search tools. This approach will save resources within the specialist ECL being used to conduct a host of more mundane queries and move this functionality directly to the investigator and/or Scene of Crime Officers (SOCOs).

EVE will improve investigative capability, better positioning Police to manage both current demand and the expected increase in electronic-related crime.

Police will implement EVE nationwide, including:

- a targeted training programme for ECL staff and frontline investigators
- a mobile EVE for use in court or for investigation at crime scenes or remote areas

Once proven, there is potential to make EVE available to other enforcement groups and jurisdictions, providing benefits beyond Police.

E-SOCO

Ensuring appropriate seizure and preservation of computer items for forensic examination is essential to obtaining electronic evidence. EVE simplifies some of these tasks, reducing the reliance on ECL specialists.

Providing trained e-SOCOs to carry out this work will ensure integrity of evidence is maintained, while reducing the lead time in making such evidence available to frontline investigators. This will also further reduce the ECL workload, enabling more focus on specialist evidence recovery.

Police will establish the role of e-SOCO, with appropriate training and procedures, enabling the seizure and transformation of electronic evidence into EVE, without involvement being required from the ECL.

European Convention on Cyber Crime

The European Convention on Cyber Crime came into force in November 2001, recognising the urgent need to pursue a common criminal policy aimed at the protection of society against cyber-crime especially, by adopting appropriate legislation and fostering cooperation between countries and private industry in combating cyber crime.

Countries signing up to the convention are required to meet legislative standards guiding the definition and response to cyber crime. New Zealand legislation appears to align with the convention's requirements; however these need to be reviewed in detail.

As well as aligning legislation with e-crime internationally, the core benefit for Police is the ability to progress cyber-based investigations across borders with other participating countries, extending the reach and speed of investigations.

Police will drive any legislative changes required and progress New Zealand's adoption of the European Convention on Cyber Crime.

The Council of Europe is made up of 46 member states.

The European Convention on Cyber Crime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the organisation.

An additional protocol supplementing the Convention makes any publication of racist and xenophobic propaganda via computer networks a criminal offence.

Non-European states who have signed up to the Convention include:

- United States
- Canada
- Japan
- South Africa

The Crime Laboratory Accreditation Program of the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is a voluntary program in which any crime laboratory may participate to demonstrate that its management, operations, personnel, procedures, equipment, physical plant, security, and health and safety procedures meet established standards.

Accreditation is granted for a period of five years provided that a laboratory continues to meet ASCLD/LAB standards.

Laboratories in New Zealand with current ASCLD/LAB accreditation are:

- ESR
- Police Document Examination Service

Integrity

The growth in e-crime places increased reliance on electronic (or digital) evidence. The integrity of digital evidence and the process by which it is obtained is essential in successfully prosecuting e-crime.

Laboratory accreditation provides Police, Courts, New Zealand enforcement agencies and their international counterparts with assurance as to the standard of forensics examination. This is particularly important in international investigations where evidence recovered by the ECL is presented in courts overseas.

ECL Accreditation

Accreditation shows that the ECL meets international standards for forensic examination of digital evidence. Accreditation forms part of a laboratory's quality assurance programme, which also includes proficiency-testing, continuing education, and other programmes to help the laboratory give better overall service to the criminal justice system.

The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) is an internationally recognised accreditation programme, based on the ISO 17025 standard.

Preparation for accreditation can be a lengthy process, ensuring that identified standards and processes are in use for:

- administration and resourcing (including budget, management information systems, job descriptions, performance reviews)
- organisational structure and delegation of authority (see also ECL and E-Crime Structure, page 8)
- evidence control and quality management
- personnel qualifications and proficiency testing
- physical layout and lab conditions (including security, design, health and safety)

Police will implement formalised standard operating procedures, high-quality exhibit management, appropriate lab conditions, and other national practices required to achieve ASCLD/LAB international accreditation.

Strategy Review and Governance

The governance of this e-crime strategy and the measures arising from it reach across many areas of policing. These include operational responses to e-crime prevention and investigation and the development of Police capabilities through training, research and resource development.

E-crime also reaches across traditional crime areas and criminal groups as well as some having new features that have emerged with the growth of the electronic environment.

The strategies in this document also affect a wide variety of Police staff and domestic and international partner agencies.

Because of the diversity of measures required to address e-crime, it is appropriate that the Commissioners govern this strategy. Key roles include:

- Executive Sponsor: Deputy Commissioner, Operations
- Business Owner: National Manager, Crime Services
- Performance Management and Review: Assistant Commissioner, Strategy, Policy, and Performance

The key elements of governance include:

- an annual progress report to the Police Executive of the strategy and its impact
- incorporation of actions into the performance management framework
- a review of the strategy to be completed by 30 September 2009

Risks and issues associated with this strategy will be identified as part of the business unit planning process and in consultation with the Risk Advisor and the Organisational Performance Group. The planning will cover strategic and operational risks in relation to services, capability, and change.

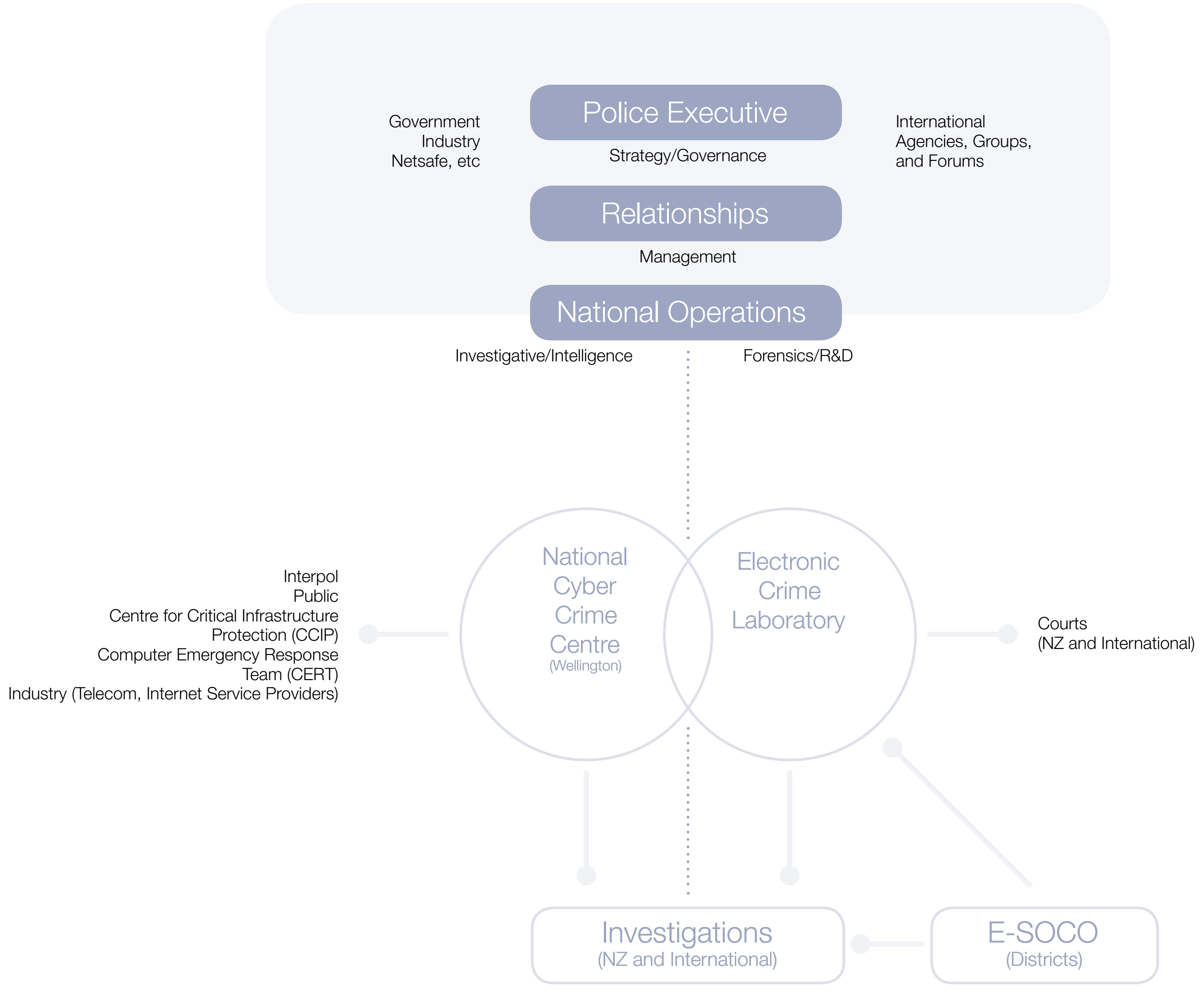
Implementation of the E-Crime Strategy to 2010 involves several key initiatives.

Additional capability will need to be acquired or reallocated by Police, to fund the key initiatives and the ongoing development and participation in key partnerships and forums.

The next steps in progressing the E-Crime Strategy include:

- prioritise initiatives and assign ownership
- agree a programme of work and associated resourcing requirements
- incorporate initiatives into annual business plans / prepare business cases as required

Appendix A: National E-Crime Structure



Appendix B: Summary of Actions

E-Crime Initiative	Actions	Timing	Owner	Success Indicators
Organisation	1. Develop, agree, and implement the national e-crime structure for the Electronic Crime Laboratory (ECL).	2007	Electronic Crime Laboratory	• national service provision with single line reporting • the ECL is responsive to District workload pressures • there is consistency of operation across all ECL facilities
	2. Develop, agree, and implement the national e-crime structure for the National Cyber Crime Centre (NC3).	2008	Crime Service Centre	• Police are responsive to requests for assistance in investigating cyber crime
Capability	3. Police will extend the use of preview clinics to each District.	2007	Electronic Crime Laboratory	• preview clinics and mobile phone booths provide investigators with results in a short timeframe • ECL staff are focussed on specialist analysis and evidence recovery, with reduced delays for investigations • Investigators are using EVE with success in resolving crimes • improved understanding of e-crime and electronic evidence throughout Police
	4. Police will implement mobile phone booths in each District with appropriate support and guidance for District staff.	2007	Electronic Crime Laboratory	
	5. Police will appoint E-Crime Liaison Officers for each District to facilitate local ECL activities and communications.	2007	Districts	
	6. Develop and implement the Environment for Virtualised Evidence (EVE), including: – a targeted training programme for ECL staff and frontline investigators – a mobile EVE	2008	Electronic Crime Laboratory	
	7. Establish the role of e-SOCO, appoint and train e-SOCOs in the identification and preservation of electronic evidence, including transformation of evidence into EVE.	2009	Electronic Crime Laboratory	• improved identification and seizure of electronic items for evidence recovery • short lead times for Investigators to access electronic evidence
	8. Review legislation alignment with European Convention on Cyber Crime, driving any changes required and progressing New Zealand's adoption of the convention.	2009	Electronic Crime Laboratory	• progress in ratifying the convention
	9. Encourage the sponsorship of research to clarify the extent, scope, and impact of e-crime in the New Zealand setting.	ongoing	Electronic Crime Laboratory	• Police have a clear understanding of the extent, scope, and impact of cyber crime in New Zealand
	10. Police will collect and analyse e-crime data, providing intelligence and direction to investigations, and strategies to address e-crime.	2009	Electronic Crime Laboratory	

E-Crime Initiative	Actions	Timing	Owner	Success Indicators
Integrity	11. Obtain international accreditation of the ECL, based on the ASCLD/LAB International accreditation programme for Digital Evidence.	2009	Electronic Crime Laboratory	• the ECL is a world class and internationally accredited forensic laboratory • consistency of practices and standards across all ECL facilities
	12. Review of the e-crime strategic plan.	2009	Crime Service Centre	• initiatives on target to achieve desired outcomes
Partnerships	**Government:** 13. Coordinate with the CCIP in responding to e-crime incidents affecting critical services, formalising requirements to collect evidence and meet other criminal investigative obligations. 14. Build protocols for effective coordination between the Customs Service, Security and Defence agencies, and the Department of Internal Affairs, through mechanisms such as Combined Law Agency Groups, the Departmental Committee on Computer Security and the Officials' Committee for Domestic and External Security, Officials' Committee for Review of Internet Security. 15. Support and contribute law enforcement perspectives to initiatives arising out of the work of the Information Technology and Telecommunications Policy Group in the Ministry of Economic Development, the ICT branch in the State Services Commission, and the CCIP.	ongoing	Electronic Crime Laboratory	• Police working proactively with stakeholders • Police are responsive to requests for assistance in investigating cyber crime • Memorandum of Understanding in place with local agencies facilitating the sharing of information and resources
	Industry: 16. Support the Internet Safety Group, which heightens community awareness and provides policy responses to e-crime issues. 17. Work with Internet service and telecommunication providers to enable access to records of traffic information to assist the investigation of crime (pursuant to search warrants). 18. Establish and maintain relationships with major technology stakeholders, eg Microsoft and Cisco.	ongoing	Electronic Crime Laboratory	• community have trust and confidence in Police • Police working proactively with stakeholders
	International: 19. Work with the Australasian Police Ministers Council (APMC) to improve the regular sharing of information, skills and response capability among e-crime managers. 20. Work with the United Nations Convention against Trans-National Organised Crime to address issues hindering Police ability to deal with international jurisdictions, including provision of mutual legal assistance, extradition, law-enforcement cooperation and technical assistance.	ongoing	Electronic Crime Laboratory	• Police working proactively in partnerships with international stakeholders • Memorandums of Agreement in place to facilitate the sharing of information and resources

Published by New Zealand Police
PO Box 3017, Wellington

ISBN 978-0-477-10059-5 (paperback)
ISBN 978-0-477-10060-1 (pdf)

www.police.govt.nz

New Zealand Government