ICTs: Tools for crime prevention?

Patrick Burton

CJCP

Safety has no boundaries

CENTRE FOR JUSTICE AND CRIME PREVENTION

CJCP Issue Paper
No. 1

April 2006

The nexus between ICT (information and communication technology) and crime prevention has been explored, superficially at least, in many forums over the past half decade. As increasing focus is placed on the digital divide and the potential for ICTs to be used to ameliorate many conditions of poverty – and as a rather nebulous route for development – so the benefits of widespread access and take-up of telephony and information technology are being mooted in diverse forums ranging from academic environments to the broadsheets.

Primarily, ICT has been identified as one of the most potentially powerful means of bringing information to previously disenfranchised and 'disconnected' communities, as well as a means of social inclusion and development within both the social and economic realms.

Concomitantly, the phrase 'digital divide' emphasises one of the innate contradictions – and potential problems – of access to ICTs: that of exclusion and shifting power imbalances between the haves and have-nots even more than is currently the case.

Yet despite the developmental potential of ICTs, the use of new technology presented by them in combating crime, the emerging forms of crime facilitated by ICTs, and the massively increased 'connectivity' that ICTs provide to previously isolated communities, little or no direct linkages have been drawn between ICTs and the prevention of everyday criminal activity.

This paper starts to explore some of these linkages, and suggests a number of ways in which ICTs can be utilised to enhance social crime prevention.

Linkages between crime and ICT

Most of the literature exploring ICTs in relation to crime prevention has focused on the implications of the new technology, and particularly the internet, for new and emerging types of crime.

As information and knowledge replace capital and energy as the primary wealth-creating assets, as information technology transforms the way that business is conducted, and as the commodities of trade are transformed, so new methods of expropriation – of 'information crimes' and the theft of ideas, knowledge and information – are developed.

The development of e-commerce whereby previously marginalised communities can now access and sell goods across global boundaries has at the same time fostered the development of new types of fraud, financial crimes and stolen identities. Theft becomes virtual and difficult to trace; fraud, strongly related to stolen identities, becomes infinitely easier to hide.

The Foresight project in the United Kingdom has proposed a number of key characteristics of import for crimes resulting from new technologies:

- The replacing of traditional communities by groups forming around common beliefs and interests may reinforce rather than challenge anti-social values.
- The dominance of ICTs may increase the ease, speed and scale of crime, and concomitantly present greater difficulty in dealing with it.
- Greater complexity in judicial systems, police jurisdictions and trans-border crime may make it difficult to present evidential trials to juries, as well as raise

DEFINING ICT

Information and communication technology is the term for the range of services that use voice and data technology to provide telephony, internet, video and other media.

Services discussed in the paper refer to those that will allow, or rather deliver, adequate access to voice and information, as well as more specialised and higher quality services that might be required for commercial and business usage.

concerns about the feasibility of presenting digital evidence in court.[1]

Importantly, there are increasing opportunities for isolation within the public space. As the Foresight project researchers argue, "business, inter-personal and entertainment activities have moved from social and static to the personal and mobile". This, they assume, leads to a dehumanised environment where people may become less real to one another, leading to more extreme reactions and interactions – a process infinitely magnified in cyberspace.

Emerging from literature of this nature, however, is the potential that new technology presents for detecting and investigating crime. Closed circuit televisions (CCT) have been used to varying success across a broad spectrum of countries, including South Africa. Techniques such as crime mapping, forensic investigations, and the sharing of information and data across borders and between agencies have captured the imagination of many.

Clearly, with new types of crime occurring in cyber environments, new means of tackling crime are needed. It is largely in this realm that most of the literature and work related to crime prevention has been done.

A Google search of ICT and crime prevention churns up some 650,000 hits, almost all of which are concerned with policing new forms of cyber-crime, or at least crimes that are committed with new technology. Issues of cyber-policing or matching police technology to fast-evolving cyber crime methodologies dominate. There is, however, very little literature that addresses crimes – 'traditional', 'conventional' or emerging crimes facilitated by new information technologies – from a prevention perspective.

A number of reasons may exist for this. First, the most common conception of crime prevention is that it is a 'responsibility' of the police and justice system, so falling into the common trap of confusing law enforcement with crime prevention. Certainly the police and other justice agents are essential stakeholders in crime prevention, but it also falls to communities and civil society to engage in crime prevention practices.

Second, ICTs are usually presented as opening a wealth of opportunities to fully utilise new and emerging technologies, and the assumption is that this can only be applied to new and emerging crimes. This, however, does not do justice to the opportunities that ICTs present in countering 'conventional' crimes – robbery, assault, housebreaking and theft – that still constitute the majority of all crimes that takes place.

ICT in South Africa

While those living in urban areas of South Africa tend to take for granted access to telephony, either through fixed-line ownership, cellular/mobile phone (cellphone) access, or even access to public payphones, much of South Africa's rural population still remain unconnected.

The latest (albeit flawed) statistics available on penetration show that 1.1 million households have only a fixed-line telephone on their premises, 1.6 million households have both a fixed-line phone in their dwelling and a cellphone, and just over two million households have a cellphone only.[2] Approximately 4.3 million households have easy access to a public payphone. In total, according to Stats SA, only 46.9% of the South African population have access to telephony. The primary reason for this number not being lower is the rapid inroads being made by cellphone operators in South Africa over the past decade. It is estimated that in excess of 19 million South Africans have access to cellular telephony.[3]

As part of their community service obligations, cellphone operators in this country have also achieved some success in reaching previously isolated populations through community and container telecentres. Many of these offer not only basic telephony but access to the internet, email and other information services, often accompanied by training.

The primary objective of such initiatives is simple, as is the premise: access to information, communication and knowledge is a fundamental right, and access to ICTs will facilitate development in a multitude of ways and spheres.

Despite this, however, the penetration of internet access into more rural communities has slowed down, increasing only 6% between 2004 and 2005 to an estimated 1.1 million dial-up subscribers.

The first step: Scope for ICT in crime prevention

The question we need to ask then is how, if at all, can ICTs be used for crime prevention; not specifically cyber-crime, but the types of crime that affect many South Africans on a daily basis. A deconstruction of the abbreviation – information, communication, technology – speaks for itself: all three elements are crucial components in any crime prevention strategy. The very tools or physical components of ICT provide the means for implementing a range of strategies and processes that facilitate proactive and integrated crime prevention.

At the most basic level, access to telephony, whether fixed or mobile, is required in order to report a crime in progress, a crime that might have been committed or any suspicious criminal activity. Similarly, radio or data connections are often required in order for alarms such as those offered by many private security companies to function.

As access to and ownership of particularly broadband internet expands into South Africa, so opportunities exist for high-speed connections to be used for house alarms and the most basic voice communication with police and security companies. Such connections are not, as often assumed, necessarily dependent on the penetration of fixed telephony.

The most well-known service model is that developed by Grameen Bank in Bangladesh for micro and small-scale entrepreneurs, where mobile signals are used in extremely rural communities. Similar models have been developed in India and in other parts of Bangladesh, as well as by rural telecentres in South Africa's Limpopo and Mpumalanga provinces. Such technology can link communities and households to police where physical access is limited. A significant by-product of this is that access to telephony can also increase feelings of safety – an important process in a country where the majority of households feel unsafe in the areas where they live.[4]

Concurrently, the personal computer is no longer the only way to access universally networked information. People are therefore not necessarily constrained by access to landline technology and to dial-up connections. As third-generation mobile technology and GPRS (general packet radio service) spreads throughout South Africa, information can be shared across PDAs (personal digital assistants), cellphones and other hand-held devices making access to and dissemination of information even easier, quicker and more accessible. This is a significant factor as cellular telephony continues to spread rapidly into previously 'un-communicated' geographical regions.

As the previous discussion reveals, a large percentage of the South African population do not have access to ICTs within the home and depend on community access through telecentres, multipurpose community centres and other public initiatives. Such facilities can themselves provide an important instrument for crime prevention. Programmes have been established in various areas in the United States to use the internet to distribute important information relating to crime prevention, and similar initiatives are under way in Kenya.

Centres of information such as community or telecentres serve a dual role: information can be distributed and collected online, and this can also be disseminated through noticeboards within the establishment, as well as through other activities run from the centre.

Examples of the types of information relating specifically to crime prevention include the identification of crime hot-spots in the areas served by the facility, lists and photos of missing or wanted people, and information on practices such as target hardening, safer behaviour or on how to

Clearly, with new types of crime occurring in cyber environments, new means of tackling crime are needed.

make one's general environment safer. Such information can be easily and regularly updated online by the police and other law enforcement personnel. This is, it should be noted, already being undertaken by private security companies operating in specific areas throughout South Africa – but on a very small-scale and clearly targeting upper-income families rather than the majority of the population.

Online communities form around shared interests, hobbies, situations and other commonalities, that themselves create a sense of social inclusion that is often otherwise missing in people's lives.

The opportunity also exists to bring communities into closer contact with the police, taking the concept and practice of community policing one step further. The internet can serve as an interface between police structures and community members. Questions can be asked of the police by the community, and concerns and fears raised. Problems and complaints can be filed online and can be directed straight to the police station concerned.

This is, however, dependent on the availability of resources within the police to manage such processes; but as ICTs and digital systems penetrate into police stations themselves, such responsibilities could be allocated to community policing officers or to others within the station who are engaged with community structures. Furthermore, this interface provides a good medium to encourage reports of misconduct, corruption or 'whistle-blowing'. Anonymity is guaranteed and many people feel safer using the relatively anonymous medium of email or the internet.

These systems are certainly not intended to replace face-to-face contact with police, but rather to supplement and make access to and interaction with the police that much easier. Such processes provide a rather more grounded meaning to the phrase 'cyber-policing', which has evolved in response to cyber crime in particular.

ICTs as exclusionary or inclusive

While the argument has been made that information technology can in fact be used to heighten levels of social exclusion – and certainly the potential exists to broaden the gap between the haves and have-nots (see the digital divide debate) – the converse is also true.

Online communities form around shared interests, hobbies, situations and other commonalities that themselves create a sense of social inclusion which is often missing in people's lives. Those perceived (by themselves and others) as 'disconnected' and marginalised can form new bonds and relationships premised on commonalities.

Ongoing discussions in sociology, psychology, anthropology and criminology literature refer to the breakdown of families, communities and social capital: the internet provides an important means of consolidating those who might otherwise feel isolated. It can serve as a 'greaser' in the way that cohesion around alcohol and drug use does, with far less negative effects and concomitant anti-social behaviour.

This is not to say that the results are all positive. The rapid growth of cyber-crimes and access to anti-social content such as pornography cannot be disputed and suggests the need to foster positive and productive online interactions, engagements, networks and communities that can at least work to counter such delinquent behaviour.

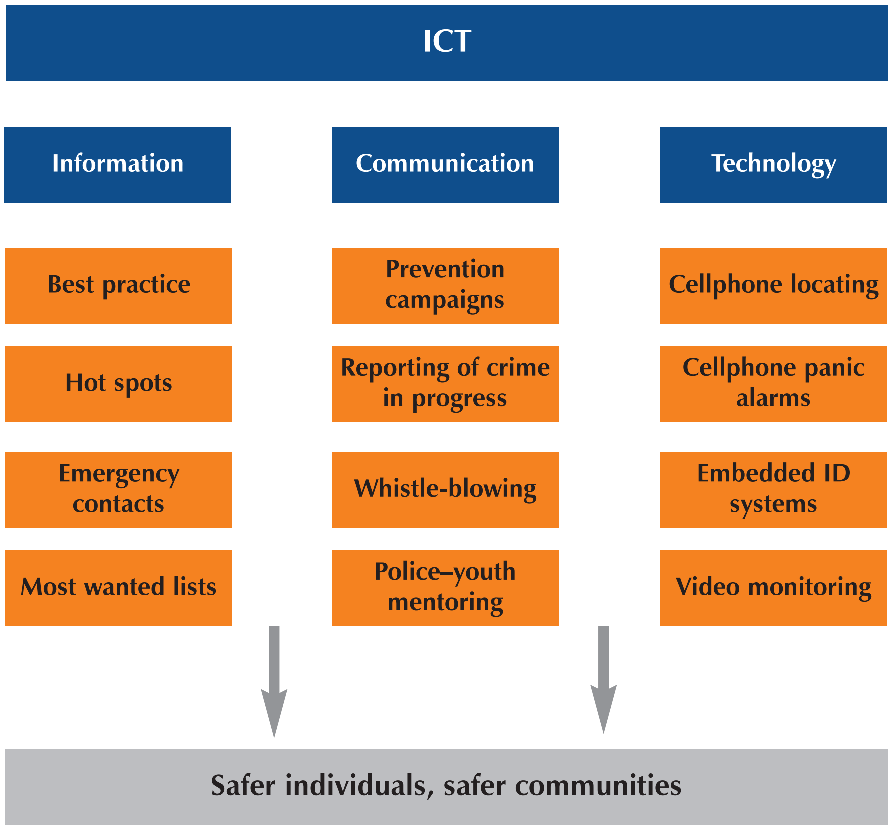
Communication for social change

Communication for social change is a relatively new (in relation to the rest of the ICT development arena) field and is a broad concept referring to the use of communication technology for developmental change. Capobianco refers to it as covering "a variety of concepts and strategies such as: communication for development, development communication, social marketing, 'edutainment', 'infotainment' or enter-educate, participatory communication, etc.".[5]

Such a definition, while broad, captures the variety of approaches that currently utilise ICT as a vehicle for change within developing societies, as well as the variety of ways in which it can be used as such.

One of the best examples of the way in which ICT can be used as an agent of social change is in the HIV/Aids sector. Using facilities such as community telecentres, service providers within the sector have

Figure 1: Comprehensive use of ICTs for crime prevention



ICT

Information	Communication	Technology
Best practice	Prevention campaigns	Cellphone locating
Hot spots	Reporting of crime in progress	Cellphone panic alarms
Emergency contacts	Whistle-blowing	Embedded ID systems
Most wanted lists	Police–youth mentoring	Video monitoring

Safer individuals, safer communities

exploited the opportunities available to extend their outreach, awareness and advocacy campaigns to often hard-to-reach populations, as well as to one of their key audiences – the youth and young adults. Information is made available on community-friendly websites on such issues as how to prevent transmission of HIV/Aids and sexually transmitted infections, how and where to undergo voluntary counselling and testing, as well as a range of other information crucial to dealing with the epidemic. In addition, community telecentres are used to display posters and events dealing with HIV/Aids.

Such media – together with more conventional forms of information technology such as visual, audio and print media – have been shown in a number of instances throughout the developing world to be among the most effective tools for the widespread dissemination of information for developmental purposes, as well as a way of mobilising communities and individuals to practise more responsible behaviours.[6]

Enhancing service delivery through ICTs

There is also a secondary, more indirect link between crime prevention and ICTs, namely, that provided through the opportunities for enhanced delivery of basic services including housing, health, education and welfare services.

These are fundamental components of crime prevention through social development (CPSD), or social crime prevention: an approach that focuses primarily on those most at risk within communities.

CPSD recognises that by addressing the risk factors which contribute to pushing and pulling individuals into crime – what are known as the correlates or causes of crime – prevention is enhanced. The most common examples include:

- inadequate living conditions such as poor housing, water, sanitation and other services;
- family factors such as family poverty, family size and poor parenting;

There is also a secondary, more indirect link between crime prevention and ICTs, namely, that provided through the opportunities for enhanced delivery of basic services including housing, health, education and welfare services.

LINKING THE CORRELATES OF CRIME, CRIME PREVENTION AND ICTs

One of the primary correlates of crime that has remained constant in criminological theory is an unstable home model – often single-parent households – linked to a lack of available role models.

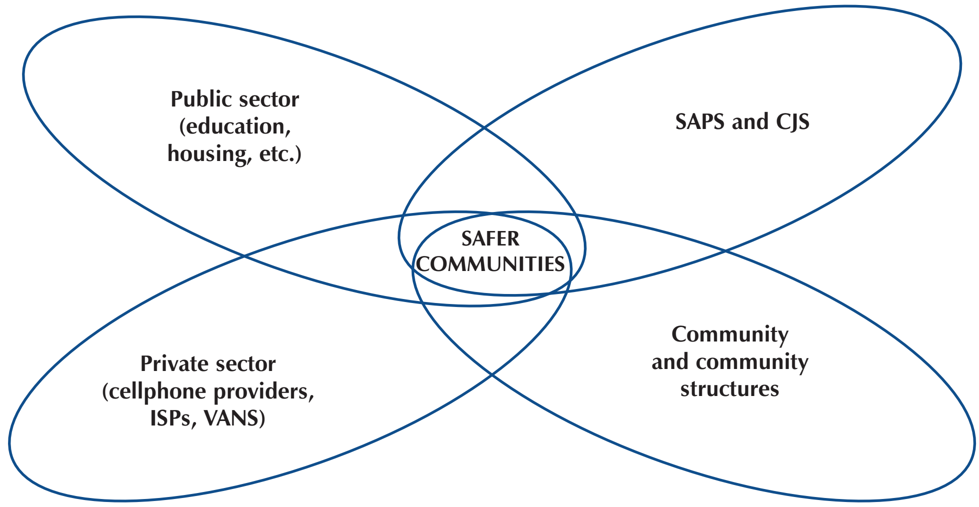
Young people within such households are considered to be at increased 'risk' of engaging in criminal or anti-social behaviour.

A pilot project in the United Kingdom is identifying young, single, pregnant mothers usually in depressed socio-economic environments.

These women are then visited by social workers who provide assistance on parenting techniques, and offer advice and other available support.

This process is intended to decrease the risk of bad parenting or unstable home environments, thus reducing the risk of the (as-yet unborn) child falling into anti-social behaviour.

Figure 2: The nexus between all role-players



- negative peer association such as networks with friends who themselves engage in criminal activities;
- school-related factors such as lack of attendance, inadequate infrastructure, truancy and exclusionary policies; and
- employment opportunities such as lack of training and employment.[7]

New information technology is increasingly being used in the delivery of basic services to society, including health care, education, water and sanitation, and welfare. For example: distance learning is facilitated by streaming audio and broadband connections; computer literacy is being prioritised as part of the process to address unemployment; other forms of information technology are being used to make public grants and welfare more available to greater numbers of people; and those living in rural areas are able to access markets and information essential for the more efficient and productive use of resources and enterprises.

Open Source Software, as a platform, has been responsible for the development of new systems within the Department of Health that are making health services more accessible to people. Information on a range of government services are now available online, increasing knowledge and accessibility. Applications for grants, funding, licenses and a range of other facilities can now be made online on, for example, the Department of Trade and Industry websites. Such accessibility facilitates entrepreneurialism that is essential for uplifting large sections of the population who currently live in poverty.

The possibilities for enhanced service delivery through ICTs have been recognised at myriad levels: 'e-government' therefore acts as an enabler, increases efficiency, maximises resources, and ultimately frees up money to be directed at more concrete, physical service delivery, while increasing access by communities and individuals to government services and information.

Even within communities, ICTs have the potential to link rather than isolate households. As walls are built higher where there were previously no walls and as households become increasingly insular from neighbouring households, so the opportunities to connect with neighbours and friends within a community through cellphones present themselves. Cellular technology has facilitated connectivity within and between communities that previously had no access to telephony or other information services; a neighbour becomes just a speed dial away in the case of an emergency, or the police just a dial away when suspicious noises are heard from a property next door.

Where to from here?

The integration of ICTs into the delivery of the most basic of services by government, as well as adopting a more innovative approach to service delivery, allows for the enhancement of four pillars of sustainable crime prevention at community level: knowledge, skills, resources and development. The use of ICTs at all levels allows for a nexus between the roles of the private sector, public sector service delivery agents, the police and criminal justice sector (CJS) as a whole, and the community in a coherent way that can only serve to enhance crime prevention at community level.

The private sector – specifically cellphone operators, internet service providers (ISP) and other value-added network service (VANS) providers – together with the fixed-line provider and the soon to be realised second operator, can provide and integrate the technology required at an individual and community level; the public sector can continue to move towards e-governance and to integrate new technology into its provision of basic services; and the South African Police Service (SAPS) and the CJS can fully utilise the opportunities provided through ICT to engage and mobilise communities towards creating safer environments.

This is, however, a process that is dependent on the buy-in of all role-players within the ICT sector, and not least on the penetration and accessibility of ICTs to all sectors of the population, including the most rural.

While advocacy for increased access to ICT and stricter requirements for community service obligations have traditionally been the domain of those directly engaged in the ICT lobbying sector, the potential of technology in providing an additional layer in crime prevention methodologies suggests that this advocacy agenda needs to be included on the agenda of crime practitioners and researchers as well. ■

In countries like South Africa where there are simply insufficient public sector resources to provide for such a service, ICTs can be used to disseminate information, provide a communication forum and offer an essential means of contact and support between identified mothers-to-be and social workers or other support structures, thereby facilitating similar interventions but in a manner more suitable to resource-hampered environments.

Endnotes

[1] Davis R & Pease K, Crime, technology and the future, *Security Journal*, Perpetuity Press, 2000, pp 59-64; Foresight Panel, *Crime: Turning the Corner*. Findings of the Crime Prevention Panel. London: DTI, 2000. <www.foresight.gov.uk>

[2] Gillwald A, Esselaar S, Burton P & Stavrou A, *Towards an African e-Index: ICT Access and Usage*, I, Chapter 9: South Africa, 2005.

[3] Ibid.

[4] Burton P, Du Plessis A, Leggett T, Louw A, Mistry D & Van Vuuren H, *National Victims of Crime Survey: South Africa 2003*. ISS Monograph No 101. Pretoria: ISS, 2004.

[5] Capobianco L, *Communication for Social Change: A Powerful Role for Communication in Crime Prevention*. Reflection Paper. Montréal: ICPC, 2000.

[6] See, among others, the Soul City programme in South Africa, and Dagron G, *Making Waves. Stories of Participatory Communications for Social Change*. New York: Rockefeller Foundation, 2001.

[7] Taken from *Factsheet: Crime Prevention Through Social Development*, <ww4.psepc-sppcc.gc.za/en/library/ publications/fact_sheet/cps/> (accessed 15 February 2006).

About the author

Patrick Burton is the Director of Research at the Centre for Justice and Crime Prevention (CJCP).

Prior to joining the CJCP, Patrick worked as an independent development research consultant specialising in the crime and justice sectors. In this capacity, and as a director of Development Research Africa, he has undertaken work in South Africa, Malawi, Tanzania and India.

Patrick holds an MSc from the University of Natal.

CJCP mission

The Centre for Justice and Crime Prevention (CJCP) is dedicated to developing, informing and promoting innovative evidence-based crime prevention focused on the groups identified as being vulnerable to victimisation or offending. The CJCP does this by:

- conducting rigorous research into issues of relevance to policy makers, public service officials, development partners and crime prevention practitioners;
- facilitating the implementation of crime prevention projects;
- providing sector-specific and accredited training in crime prevention for policy makers, public sector officials and non-governmental organisation practitioners; and
- disseminating the results of its research and lessons learned to relevant audiences.

About this paper

Information and communication technology (ICT) has up until now been primarily associated with crime only through the opportunities presented for emerging cyber crimes, and the possibilities for policing and detection.

This paper argues for stronger linkages between crime prevention and ICTs, and for the integration of everyday technology into crime prevention practices that can be easily adopted wherever access to the many forms of ICT exist.

CJCP
CENTRE FOR JUSTICE
AND CRIME PREVENTION

Safety has no boundaries

ISSN 1819-2661
9 771819 266017 >

ISSN: 0-620-36131-X
The opinions expressed in this paper do not necessarily reflect those of the Centre, its Trustees, members of the Advisory Board or donors. Authors contribute to CJCP publications in their personal capacity.

Published by the Centre for Justice and Crime Prevention
PO Box 44702 Claremont 7735 SOUTH AFRICA
Tel: +27 (0)21 687 9177
Fax: +27 (0)21 685 3284
Email: wendy@cjcp.org.za
www.cjcp.org.za