Policing and Use of Information Technology: An Assessment

by

Dr. Marcel-Eugène LeBeuf

Research Centre
Canadian Police College
Ottawa, 2000

Introduction

Currently, the police have to deal with a new paradigm. They have seen the gradual end of one period where, for many years, they had full control over their field of action, to a period, which is not transitory, where three new factors are to be observed simultaneously: technology-based criminal activity that has none of the characteristics of traditional crime; new high-performance working tools that require very specialized training for their use; a stronger articulation by the public at large as to the role they wish the police to play within their environment.

This document provides a summary of the various issues and problems related to the introduction and use of information technologies within the public security. It also takes into account the upsurge in a new type of criminal activity that makes use of technology and that has abandoned traditional means of the past. It examine avenues that will allow law enforcement bodies to prepare for the technological future, something they have hardly begun to do (Tafoya, 1995).

The very expression 'Information Technology' is ambiguous, general and yet restrictive. The term is used to designate a variety of more or less complex gadgets, machines and software which, as Nogala (1993) put it, have each their own specific development, use and impact. The term 'Information Technology' leads us to ask two basic questions which, though easy to express, are difficult to answer: Which of these technologies are useful to our police forces? How does the integration of such technologies change the role and task of the police?

In this document, we are looking at the development of information technology as it effects public safety. Without attempting an exhaustive overview, we will be looking at a number of key elements of these technologies, including, without priority ranking:

- information technology and the police
- integration of the technologies into the traditional police environment
- equipping the police with MIS
- technology users within a police department
- introducing technological tools
- incentives and de-incentives
- the cost of technologies
- the impact of technologies on police operations
- IT training
- ethics and liability

Information Technology and the Police

The interaction between the police and technology is complex rather than linear. It concerns both power and information. With respect to power, information technology promotes actions and secure results that were previously impossible to achieve, and thus police operations are improved (Manning, 1992). Moreover, the public image of the police and their impact on society are significantly enhanced. To this end, the Web pages published by police departments constitute an innovative exercise in public relations which allows them to inform the public of crime prevention activities in their locality, supply statistics on the level of criminality and provide an information framework with regard to missing persons (Strandberg, 1998; Haley, Taylor, 1998; Goodman, 1997; Wilsker, 1997; Anderson, 1997; Corsentino, Pettinari, 1996).

With regard to the information to which the police have access, it is true to say that technology allows the police to remain a symbol of authority within communities (Ericson, Haggerty, 1997). This is because such access, to data banks and other computerized instruments, provides them with more information and thus allows them to develop more effective strategies for combatting both traditional and high-tech crime (McLean-Lipinski, 1999). As police work, to use Manning's (1992) expression, is ecologically scattered, its sought-after effectiveness depends on a number of factors including the organizational culture of the various groups of workers, the type of information that is stored and the methods of doing so. Information

warfare is a real threat and includes money laundering, gaming, all forms of extortion including credit cards or the use of computers to falsify data, economic crimes, MIS sabotage, computer hacking, spying and other activities by groups linked to organized crime (Coutorie, 1995; Dobeck, 1997; Carter, Katz, 1998). Committing such crimes do not depend on geographic movement. Real crime and real issues are to be found in a new virtual universe which is now well established (Rosé, 1996). The new connections are horizontal and invisible (Marx, 1997). To win in this universe, you have to be the one holding the joystick. If law enforcement bodies hope to be as smart as the criminals, they will need to adopt the technological tools available on the market (Campbell, 1997). The challenge is not so much to adopt information technology as to adapt information technology that can systematically be helpful to the police in dealing with these new problems and issues.

Integration of the Technologies into the Traditional Police Environment

It is relatively difficult to chart the current use of technologies by the police. Technology has been part of the police environment for more than 150 years (Soullière, 1999). However, to date it would seem that, as a whole, this technology has been used in a transient and sporadic manner in a number of police departments across Canada. In fact, they have been aware of the utility of technologies for more than fifteen years (Carpenter, 1984). However, the technology sector market has developed at a speed that is in inverse proportion to that of public police department decision making. The police represent a potential market and one that needs to be developed rapidly. This means that the police need to learn how to determine both their own needs and those of the community they serve in order to make an informed choice of the most appropriate technological tool.

It is a well known fact that within police departments, the decision makers do not always have the skills required to make the necessary decisions (Carpenter, 1984) or even to become involved in decision-making (MacDonald; Martin, 1986) within a process whose ramifications have become less and less transparent (Loree, 1987). When it comes to information technology, the situation is even more complex, since the decision makers deal with new tools that can be very effective when properly used, but which are perfectly foreign to the traditional police environment (Martin, 1996).

In many cases, there are a number of new elements: the technology as such (e.g. AFIS—Automated Fingerprint Identification System), the link between technology and traditional work, and the ability to fully exploit this technology. During our research project, we visited a certain number of police departments. On one occasion, a police officer demonstrated the crime mapping system. At some point, the police officer admitted that she had taken more than eight months to learn how to handle the software, which clearly would have given much better results than those she obtained, if she had received the appropriate coaching and had some level of skill in data management.

This example shows that technological tools can be very effective if they have been developed specifically for the police or in cooperation with the police. The performance of these tools would appear to be a relative matter since the amount of extra information obtained through the use of the software will depend on whether or not the user is capable of fully exploiting its potential. Most of us who have used word processing software such as *Word Perfect* or *Word* will recall that they only discovered the fine points in these applications after several years of daily use. The performance of any apparatus will vary according to the way in which the user exploits it. However, one should not forget that all software has built-in restrictions that come into play when integrated into a larger technological whole.

Equipping the Police with MIS

New technologies will put a fresh face on the services offered in order to meet the needs of the tax payer (Audet et al.,1996). They will contribute to transforming the police into a body that is truly at the service of the citizens, a community police force, as it were. The population looks at the money that is pumped into the public domain and demands a higher level of performance from the services they are supporting (LeBeuf, 1998). But the need of the users, in this case the police, must also be met as they gradually

move from being a traditional reactive force and become a more pro-active service. To deal with this problem, the Sûreté du Québec (community relations activities) has developed a reference tool, the ARC project, that records every police intervention within the framework of crime prevention.

To meet client needs, the organizations have set up intelligence structures that allow the police to intervene rapidly, effectively and autonomously in their local neighbourhoods. Currently, a number of police departments are equipped with technology such as the AFIS (Automated Fingerprint Identification System*)* for fingerprinting, or the GPS (global positioning system) for communications, or even mobile data computers. We still need to construct a more detailed chart of the situation of the police forces on a country-wide basis. We should also mention that, internally, the relationship between superiors and subordinates is changing, thanks to the new level of autonomy acquired and experienced by employees who have more direct access to data banks and, consequently, to the potential for strategy updates.

However, the private security market, which is innovative and primarily concerned with the protection of property, has developed and uses tools that are often well ahead of any system that public security organizations can afford. It won't be long now, certainly not a question of decades, before the major areas of protection, whether of places, property or persons, will be ensured not by human beings, but by robotics, satellites, nanotechnology and micro-engineering *(*Moore, 1995; Akrich, Méadel, 1993). Moore (1995:2) describes security zones that can now be protected by invisible movement-sensitive light rays or by laser or pulsers. Robotics has also an exceptional role to play in laboratories, thanks to the delicate handling operations which it allows when, for example, extracting chemical compounds (Johnson, 1997). Biometrics, a technology which brings together finger prints, palm prints, specific features of the face, and readings of the retina or the iris, will constitute the future identification system. In the same way, DNA (deoxyribonucleid acid) identification will become commonplace. Indeed, the Canadian Parliament has adopted the *DNA Identification Act* that authorizes the setting up of a DNA data bank for genetic identification of persons convicted of serious crimes.

Technology Users within a Police Department

There are as many technology users in a police department as there are tasks to be accomplished. It is not the same person who uses a crime mapping system or a mobile data computer. In the first case, it is the analysts who have access to the software and whose task it is to obtain as much information as possible for the benefit of investigators and of patrol officers. But investigators and patrol officers themselves do not have either direct or even limited access to this tool. In the second case, however, the patrol officers deal with the information directly in their patrol car. They access the material that allows them to work better and which simplifies their tasks often by getting rid of all the paper work.

Overall, and this will simplify our demonstration, we could classify users into four main types: the executive, the investigator, the patrol officer and partners. However, one should remember that any form of discrete classification also eliminates the complex aspects of the demonstration.

Senior executives, or those in charge of teams, are looking at a lessening of financial and human resources. They will be required to look to improved technologies in order to carry out their tasks in a different manner (Morrison, 1996). But executives have been trained in their work with methods from another era and in a pre-technological environment (Rodriguez, 1995). Today, they have to articulate their needs using their own understanding of technological tools, by taking a technological standpoint that corresponds to the strategic and corporate vision of their organization. They need to create flexible organizational structures to manage both the work and the individuals, to encourage horizontal cooperation between the units and, most of all, to understand and control a decision-making process based on skills and not on rank (Martin, 1996).

Moreover, the organized crime or computer crime unit investigator is now required to understand and use new tools to deal with the challenges of this type of criminality. Henceforth, investigators, search warrant in hand, are less likely to confiscate ledgers or other pre-MIS documents. They will be looking for PCs and hard disks, and will be intercepting encrypted cell phone communications. In other words, they will be dealing with the world of communication technology that affects society as a whole, but which is also used for criminal activity.

Analysts, for their part, can now access an enormous number of data banks that offer material for their work. How can they make a proper choice of material, taking into account the needs to be met? One of the first consequences of accessing such a vast amount of material is that analysts must learn to think differently. Rather than concentrating on a single problem, they will need to develop the ability to think up several problems and several possible solutions at the same time, and sometimes collaborate with colleagues scattered across the world, whose experience and language are different from theirs (Dorn, 1998). Like everyone else, analysts find themselves faced with too much information. Data will have no significance unless it is transformed into a language that is meaningful for operations and/or management. These new tools necessarily change our ways of looking at crime and analyzing it. The VICLAS (violent crime linkage analysis system), for example, which is used in the case of serial murders, totally changes the investigators' use of their accumulated data (Sheptycki, 1998). Could unlimited technology become a hindrance for the police because of the difficulty in processing it all?

Depending on their department, patrol officers are now using patrol cars that have been transformed into mobile MIS laboratories. On the one hand, a number of boring repetitive tasks have been simplified thanks to data banks and software. Nevertheless, patrol officers still learn to manage and coordinate the technology on board, whether it be the camera that photographs them when they leave their car, the mobile data terminal, lap-top, or the mobile data computer, E-mail and so many other tools. These items improve police safety and police performance (Parsons, 1993). It is believed (LeBeuf, 1999) that tomorrow's patrol officers will be community based. This remains to be seen, but they will certainly be technology-based.

Moreover, since information technology generally eliminates a certain number of tasks, one could imagine that there will be a sense of collegiality and cooperation between colleagues and MIS specialists. As we have already mentioned, we need to get these specialists out of their offices and encourage them to cooperate with police officers in order to adapt technology to their needs. The MUCPD engineer in charge of developing MIS has insisted that front-line police officers should be involved in his work structure so that the systems developed meet their needs.

However, contrary to what is generally thought, technology confines individuals even more closely within the perimeters of their tasks, demanding a high level of competency and the development of a cutting-edge skill. Once analysts have learned to handle crime-mapping software, for example, they will begin to discover the full potential of the tool. In other words, individuals achieve a high level of performance not so much as police officers, but as experts in the management of a piece of software. This restructuring of their working approach leads them to understand and define the reality of crime in its full complexity, thus eliminating simplistic explanations (Catalyst, 1996). If you transfer such individuals, then you will create new training costs and, more especially, an indecisive period where the analysis of criminality will not be carried out at the same level of competency as previously.

Finally, we must look at another category of users, who have a very specific relationship with technologists. We are talking here of industry and government which themselves may be involved in partnerships with the police. Reports of various experiments in US partnerships of this kind indicate the advantages for the police of cooperating with major private industries (Fulton, 1995), or with government services such as the army (Smietan, Ferris, 1996; Preimsberger, 1996). Research into non-lethal weapons has had major impact on police work, giving rise to technologies such as the *smart gun* or the *sticky foam* (a spray that immobilizes a dangerous suspect), the *road patriot* (which stops a vehicle by disconnecting its electrical system), imagery process mirrors (developed by space researchers to significantly enhance blurred or inaccurate images), and the *GPS* that provides patrol car latitude and longitude and allows them to be located rapidly. The Collines-de-l'Outaouais Regional County Municipality police department, that operates over a vast rural area, uses this technology to provide a greater margin of safety for its personnel.

Another form of partnership is based on the possibility of exchanging information between the police and community groups through the use of a more effective information system (Catalyst, 1996). The premise is that the police is not the sole depository of information concerning life within the community, and constructive exchanges can easily be envisaged through the use of various technologies. The question still remains as to how to ensure that the use of technologies enhances the ability to systematically diagnose social problems (Sloan, 1996).

We should avoid making hasty generalizations at a time when the police forces are often still learning by trial and error how to handle instruments that are new to them and that were not included in their original job-training process.

Introducing Technological Tools

At the beginning of the 1990s, a major police department decided to adopt the new forensic identification technology. The process, which lasted five years, allowed the implementation of the AFIS and eliminated a great number of forms and documents from the files. This was the beginning of the paperless era. However, these five years of major change had their ups and downs. The operation had been planned out on paper, but a certain number of major problems developed during the process of change: suppliers went bankrupt; certain data bases could not be activated because of incompatible platforms; the systems sometimes went down while manual data contained in files was being transferred to computerized data banks, arousing a great deal of critical comment. Finally, the destruction of old files led to extremely violent reactions from the employees whose handwritten notes were destroyed. Once the process was completed, the system required only two work stations compared with the previous twenty-eight.

Consequently, one of the major difficulties faced by the executive is to develop a business plan to meet the daily needs of the process. However well change is planned out, it will not give good results if it does not take into account simultaneously the development of tools, of mentalities and of the factor of resistance to change. Technology is handled by men and women exposed to diverse levels of stress because of their police work, and because of the professional framework in which they operate. The degree to which the hoped-for results of technological innovation are achieved will depend as much on one as on the other factor.

Moreover, the introduction of MIS also requires the ability to take in experts to look after the running of the system for the short or medium term. It is quite fascinating to note that police departments have taken in experts from computer companies or have created positions for civilians, computer engineers, computer technicians, etc. to ensure the proper management, planning and replacement strategies related to the new systems. The new creative spirit within the police department (Pitcher, 1995) is the computer technician or technology manager. The police, consequently, is welcoming highly qualified specialists, not so much as managers of scientific areas such as laboratories, but rather in order to plan out and develop advanced computer programs for their whole staff (for example, mobile data computers) (Breton, 1996).

It happens that the product offered by a company does not correspond exactly to the needs of the police. We should then look at developing, along with the company, a product that does meet these needs. As we were told, Aif a product does not exist, we will have it made, but that supposes an enormous level of involvement. This, however, is not the role of the police, but of researchers who, aware of the complexity of police work, set out to design new tools. The role of the police is to adapt the appropriate technology to its own needs. With this new strategy in mind, we will call on the police to cooperate with experts rather than to play the role of experts themselves, as they do traditionally. This means that the police will adapt their normal work methods on the basis of their own ability to handle the high-performance tools available to them. It should be noted that, although their tasks will be refined and simplified by technology, the final result may not be greatly enhanced. New technologies do not create competence or experience.

Incentives and Disincentives

How does one make it easier for a police organization to adopt a technological approach? Nogala (1993) identifies the internal and external incentives and de-incentives. Let us take a look at them.

Internal incentives result from factors at different levels. One, for example, is the improvement of performance in the application of the law and in cooperation between police departments. The incentive may be to combat major banditry, day-to-day criminality and the fast developing area of technological crime. It is in this last area that we find the new types of crime linked to the use of technology, an area which is still difficult for the police departments to handle. Consequently, the orientations or strategies favoured by the police will promote and accelerate the use of technology and integrate it more and more

into the system as a whole. There are essential conditions to be met in order to do this, including the ability to pay for the technology and the ability to integrate it into the working environment. It will also be necessary to strengthen cooperation between police forces, cooperation which may, for example, involve the use of special squads, like *Carcajou,* which was set up to combat organized motorcycle gangs in the Montreal area in the mid-nineties and which brought together police officers from the Sûreté du Québec, the MUCPD and the RCMP. Cooperation of this kind facilitates rapid exchanges, adequate communication and information sharing. We still need to assess how, in fact, the information exchange process works, particularly where information technology is not compatible.

There is a second, rather different factor involved. The police are involved in a definitive professionalization and specialization process. Investigators dealing with organized crime have had to add to their working tools the use of the ACIIS II, an automated criminal intelligence information system, which allows them to identify the position and role of criminals within organized crime (Kerr, 1999b). The introduction and full use of cutting-edge technology require that the users have highly specialized technical qualifications. Should we, therefore, train personnel on-site so that they can fully exploit the potential of these technologies or should we bring in experts who not only can handle the technology, but can also monitor the rapid process of changes in the area? More generally, the issue is the strategic vision to be developed by police departments, in order to meet the needs of their communities and of the members of their departments. They must also be able to make informed decisions as to the technologies they select, so that such technologies do not become obsolete too rapidly.

A third factor worth bringing out is that these new technologies appear to be effective weapons of incredible potential. For example, the *compstat*, following its initial testing out by the New York police department (Bratton, Nobler, 1998) has developed into a strategic tool for neighbourhood crime management and has also helped project an image of the police force as being active both in prevention and repression (Green Mazerolle, Haas, 1998). It has got to the point where advanced seminars are being held on just this subject. This means that the police are perceived as able to solve more problems and to maintain their power of social control through the use of technologies placed at the service of the community (National Institute of Justice, 1997).

External incentives are linked to technological progress and rapid social development. One of the new and irresistible driving forces is the incredible speed with which both current and developing technologies are changing (Castells, 1996). The innovative cycle has become very short, equipment has become more powerful and cheaper, as complex processes are transformed into day-to-day tools. After two or three years, an MIS is often out of date or no longer compatible with other computerized systems that have been acquired since the initial installation. This means that police departments are likely to find themselves faced with one or more of four problems: they may be overtaken by the technological market; they may lag behind the most recent developments; they may be hindered in their development by the fact that their systems are no longer compatible, or they may be unable to expand because they lack the financial resources to upgrade the systems they do have. The technological market is knocking on the public security door, having first saturated the private security market which, as we have already mentioned, is less and less people-dependent (Moore, 1995). Moreover, the security needs of individuals and private commercial interests had led to a search for technological solutions to security problems (Boullier, 1993; Clarke, 1993). The development and introduction of video surveillance is no longer exclusive to private security, but has become a working tool for public security services as well (Ocqueteau, Pottier, 1993).

Disincentives to progress are numerous and relate to several factors concurrently. As of now, the police will be using more and more sophisticated and costly equipment. However, there is a clear gap between what we hear from engineers and specialists and the daily experience of police users. Technology does not always carry out its promises and sometimes makes only a slight difference. In fact, if we can make a simple analogy, having a word processor isn't enough to make you a writer. Technology becomes effective when a certain number of ideal conditions are met, such as proper training, backing by experts, in-depth knowledge of the use of the apparatus. Sometimes technology only becomes really useful after expensive adaptations.

Another important and determining factor is the limits of police financial resources. It is not possible to finance all the desirable technical options and all the products available on the market. Direct and indirect

costs are high and recurrent. The purchase of an apparatus now means that in the relatively short term, i.e. after a few years, it will be necessary to change or to upgrade it. Likewise, the development, research and maintenance of technological skills are relatively costly for the police, which means that even today these technologies are often not seen or perceived as a priority. Moreover, since it is necessary to develop and adapt training for each change in the technologies used by the police, immediate and direct costs ensue. The police have moved into the era of permanent and ongoing change.

Another important aspect of the changes created by technology, which is proving to be a major and complex obstacle, is the situation of the police forces around the country. According to the Canadian Constitution, police forces, with the exception of the RCMP, come under the jurisdiction of the provinces. This means that there is a fragmentation of the overall police entity that is difficult to deal with when trying to develop national standards. Moreover, the various police departments tend to go their own ways and don't have a natural impulse to get together in order to create a critical mass, for the purchase of material, for example. This means that it is very difficult to ensure compatibility of the technologies that have been developed by different companies. Finally, small and medium-sized police departments do not have regular on-staff experts who can assess the technologies, the aappropriateness of purchasing and ensure strategic planning of the technology to be acquired (Brady, 1996).

The Cost of Technologies

It is difficult to determine the direct cost of technologies. Do these costs only cover the apparatus or the software, or should they also include costs linked to personnel training, to the restructuring of human resources and system security?

There are recurrent costs related to the purchase and upgrading of apparatus and technological tools of all sorts. And budgets should take these into consideration. Then there are hidden costs linked to the introduction of the technology. They include the expense of recurrent or prolonged sick leave taken by individuals who resist change or wish to sabotage it. Another problem is that of demotivation and apathy, factors that are more difficult to evaluate, but are nevertheless significant and which can contribute to the costly failure of a technological venture.

Another cost factor is the training of both personnel and senior executives. Though the issues and training costs may be complementary, they are nevertheless different. It is indeed astonishing that there is so little literature regarding the training of top-level executives within the field of information technology or on the type of information required for the development of a strategic vision and an informed decision. However, training is a constant priority and subject to continuous upgrading. Tomorrow's training programs must be developed bearing in mind the concerns and needs of tomorrow. Again, a wider vision is needed to compass the new issues raised by technology.

Finally, technology security itself raises significant and costly problems B problems to be resolved and problems to be eliminated. If there is a general consensus that information technology substantially enhances the effectiveness and performance of police users, what is perhaps less well known is that, as we shall see later on, the same technology increases public vulnerability (Grabosky, et al., 1996). Examples of this vulnerability are the development of new crimes such as telemarketing fraud, embezzlement of electronic transfers, illegal tapping of cell phones and electronic vandalism. In the latter case, we refer to a virus attacking the MIS in the same way that viruses attack human beings. It costs an enormous amount of money, not only to protect oneself against illegal attacks and invasions, but also to reboot the weakened or destroyed system (EDP Security Bulletin, 1998).

The Impact of Technology on Police Operations

The impact of technology on police operations is various and varies according to the sectors concerned. The opening hypothesis is that technology is integrated into police work on the basis of the benefits that they will engender for police operations. This hypothesis remains to be proved. Within the information technology sector in particular, one can identify three major forms of impact.

Recourse to technology increases the effectiveness of one's work by eliminating or reducing the number of repetitive tasks, in particular for patrol officers. This leads to an improvement in performance, more rapid response time and a higher solution rate (Seaskate, 1998, Lingerfelt, 1996). By transferring some part of the administrative tasks of the police officer to civilian personnel, patrol officers have more time to devote to their community. Again, in the field of forensic identification, the fact that one can access computerized files that already contain basic information, significantly reduces the time needed to complete electronic forms. There are less repetitive actions required. Moreover, the information obtained is of higher quality, since police officers can immediately check out the data banks and, where necessary, fill in missing information.

Technology opens the door to the installation of an extended communication network which has a high performance level and interconnects departments that otherwise would not be in touch. However, one still has to assess the quality of these contacts and the results obtained by the new network. An analyst working in a major police department reports that she was able to contact a large number of analysts and investigators in her department thanks to E-mail and the Internet. However, she also noticed that if she used the telephone, she was able to develop stronger and more personal relationships, which worked in her favour when it came to long-term information exchanges and cooperation. Direct person-to-person contact meets the need to set up a real network of more humane contacts and thus to obtain more accurate and specific information. A more superficial contact created by E-mail comes in handy when you need only general factual information.

The setting up of high performance (or significant) communication networks has an immediate ripple effect which modifies decision-making practices. It means that a police department that wishes to tie in with a powerful high-performance system needs to have equipment that is compatible with that used in other departments or in the major regional departments. The transfer of information and knowledge collated in data banks is more and more dependent on the transfer of technology. From this point of view, information technology generates improvements in working techniques, but it does not replace them.

When police officers work with information technology, there is less emphasis on the evaluation of the task in terms of performance or quantitative results than on the ability to work through different sites with multiple connections. New work divisions are based on the capacities and skills of the worker rather than on the task. For example, forensic identification teams are now much smaller, but their work is completed more rapidly and more accurately, with fewer personnel. Police officers in the forensic identification program do not inevitably work faster than formerly. This is not necessarily what is asked of them, but the Identification Section offers more effective overall results since a large number of repetitive tasks no longer need to be effected thanks to the inception of computerized data banks.

IT Training

Police training has been transformed with the introduction of technology. Not only is there a prime need to train people in the use of this technology, but technology itself is used to provide training. Here we are referring to the development of distance training (Wells, Minor, 1998). Staff are trained in accordance with their needs and using electronic contacts including Internet (Myers, Myers, 1998) and at some future date intranet (Kerr, 1999). Individuals may access teleconferencing or training programs assisted by computers or CD-ROM (Hutchison et al. 1998), or make use of firing range or driving simulators to allow learners to experience situations that are as close to reality as possible (Pilant, 1994). One Canadian experiment in the training field is *Athabaska University*, a virtual university which has no campus but trains students.

We have referred several times to the needs for training to be priorized within the fundamentally changing context of police work and technology. Indeed, technology means that apparatus and data banks are more powerful, that the ability to swap information has been multiplied ten times and that interconnections between the systems, police departments and data banks are easier to make than ever.

The inevitable question is whether technology is creating a new police profession. If so, then one would need new material such as that now being integrated into police departments, the recruiting of personnel able to handle tomorrow's police tasks and a training that will ensure the optimal use of the instruments to be used by the police officers. Training, necessarily, will become specialized and high level in order that

trainees may understand the operational side of the technology and meet community needs. This is something that the French government noted during the national training conference which took place in February 1999 in Paris (France, 1999).

MIS technicians and systems specialists will be required within the police force. A small police department like the one at Hull, in Quebec, which has a payroll of about 100 police officers, hired a computer technician five years ago as a full time employee. He manages the networks, plans out changes to current technology, reboots the system when it goes down, designs new computerized applications and looks after the management of the area. He also ensures that the systems meet maximum security criteria in order to protect the police information service. And he tries to ensure that the systems selected by the department are compatible with those of other police departments.

Ethics and Liability

There can be no area where it is more necessary to scrutinize the ethical side of police activities than when it comes to using technology. Indeed, it is true that for a considerable time now we have accepted that a computerized system such as the Canadian Police Information Centre (CPIC) must be protected because it contains a great deal of information on individuals. This also means, given the ease of interconnection and the speed of existing software, that it is essential to ensure that police accessing this type of data bank, to input and extract information, should use it exclusively within the framework of their mandate (Marx, 1998). A commission of inquiry recently revealed that police officers had used data obtained from a data bank for personal ends (Sûreté du Québec Public Inquiry Commission, 1998). Something that is unacceptable but exceptional may turn into an everyday habit if an ethical reflexion on technology and its use is not begun and pursued. Technology must not be used for purposes for which it was not designed. We should remind those concerned that ethics should be part of the daily life of all police officers, whatever their rank, function or the extent of their personal ambitions within the police force. The ethical approach which is first presented in the classroom should be maintained and encouraged in the police officer's daily activities. It would also be salutary if unethical behaviour were reported, but this seems still a lot to hope for in the light of contemporary police culture.

Another issue is that of the liability of police departments when they use technology and the legal proceedings that may ensue. The use of non-lethal weapons such as cayenne pepper (oleoresin capsicum), which is permitted because it constitutes an alternative to regular weaponry, has led to court proceedings in the United States which resulted in the conviction of police officers who used pepper sprays against a rambunctious offender (Cansler, 1998). Again, intercepting private communications when access is prohibited by the use of keys raises the question of the right to privacy and the right to the protection of the public at large (Cansler, 1996). However, one thing is certain: technology should not be improperly used or used for purposes for which it was not intended.

One may also suppose that the new work methods based on high-tech apparatus will allow police officers to take suspects' statements at the scene of the crime or in the patrol car, a practice that is current in the London (Ontario) police department. There, thanks to a PC which stocks the requisite forms, the suspect confirms the accuracy of his statement, not by signing it, but by clicking on the 'Send' button, which immediately transmits the statement to the H.Q. data bank. Another problem is that mug-shot files, which offer an extended choice of suspects for crime, could be a source of difficulty for crime control. Digital photos can be modified by computer without there being any trace of a change. In other words, a photograph could be modified to suit the characteristics of a suspect so that they look alike. This rather silly example allows us to stress the fact that police work is being simplified and refined thanks to the technology, but we still have to see how the law will deal with the introduction of these new techniques.

Finally, there is the major question of encrypting, which raises a number of basic questions. Encrypting is the ability to hide the content of the message by making it incomprehensible except to authorized recipients. We know that Internet was financed by the US Army during the cold war in order to increase the number of communication sources in the event of a major nuclear attack. Internet is a huge worldwide computer network, and in 1997 it was estimated that it included some 80,000 independent computer networks (Dobeck, 1997). This means that it is fairly difficult for law enforcement services to penetrate the

system. One of the solutions proposed by the United States is that government should have control over servers, a suggestion which has not been unanimously welcomed and which runs counter to the very principle of Internet and of the right to privacy (Pilant, 1999).

Concluding Remarks

A great number of the factors affecting the role of technology in the police depend to a large extent on social forces whose interaction and development are not easy to predict. The future of technology is based on strictly human considerations: a police chief who is motivated by technology, specialists who work to get a file accepted, budgets that are developed under pressure from seasoned warriors in the field. Technology is there to hand, but it is up to the decision-makers to understand this.

There are already studies on the way in which police departments collate and analyse data (types, objectives, etc.) and also how the police access such data (O'Shea, 1998). There are others in which the emphasis is on the extent to which technology diminishes the number of reports and forms that have to be drafted or filled in (Moriarty, Dover, 1998). There are yet again others based on surveys of target groups that indicate that computer crimes (copying or illegally selling software, illegal intrusion by hackers) are not necessarily seen as crimes, and particularly not by students in engineering or technology (Mercier, 1998).

If, as we have noted, the introduction of technological tools requires planning in terms of costs and modification of functions, it is still true that the development of these tools is being pursued at an extraordinary rate, as is their marketing. On one hand, police officers ask their superiors to provide apparatus to facilitate and improve the carrying out of their tasks; on the other hand, management is under pressure from the market itself, which sweet-talks them about the advantages and benefits of highly developed tools, advantages that sometimes go well beyond the real needs of the departments, or create new setting-up costs because the systems are incompatible.

There is, indeed, no rational approach to integration or use of technology. We suspect that the decision-making in this area is based on a transient rationalization supported by knowledge and skills that are external to and uncontrollable by the police itself. The lack of familiarity with the tools means that they are integrated only partially or superficially, in an attempt to make them compatible with traditional work methods. In the end, technology necessarily goes through a transitional phase where the police have to first learn to come to terms with tools that promise effective problem solving before they can integrate them and use them properly. It is essential that we do not become too independent of our suppliers and of those who control the market (Naulleau, 1998). Once the transitional phase has been completed, a phase that can be quite long, given the human and financial factors involved, it is still necessary to learn how to integrate these new tools with the classic working methods with which the police are familiar and which were developed much earlier. Since it is necessary that users be trained to adapt to the tools, and that experts be on-site or reasonably available to help or to handle the apparatus, which means reorganizing human resources, integration is like a game of leap-frog—up and over, down and across.

Not only must we prepare police departments to understand the major changes that will be caused by the introduction of high-performance technological tools, tools that are completely new within the field of police work, we must also prepare them to integrate these tools, to handle them properly, so that they do not lag behind when it comes to dealing either with new forms of crime that derive from such technology, or with more traditional criminal behaviour. It may be fairly easy to understand that computer fraud requires up-to-date skills and specialized knowledge, but one must also realize that crime control is also dependent on new tools such as remote detection (Quirion, Lamy, 1999), and that these techniques have to be learned by active police officers.

References

Akrich, M.; Méadel, C. (1993). Technologies de sécurité et organisation. *Les Cahiers de la sécurité intérieure,*21:53-59.

Anderson, P. B. (1997). Web Technology in Law Enforcement. Page web consultée le 1999-4-26.

Audet, M.; Jacob, R.; Lauzon, N.; Rondeau, A. (1996). *Renouvellement des services publics et autoroute de l'information: vers un modèle stratégique de transformation et de critères d'aide à la décision.* Version finale. Présenté au Centre francophone de recherche en informatisation des organisations (CEFRIO). Septembre.

Boullier, D. (1993). La vidéosurveillance à la RATP: un maillon controversé de la chaîne de production de sécurité. *Les Cahiers de la sécurité intérieure,* 21:88-100.

Brady, T. (1996). The Evolution of Police Technology. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Bratton, W.; Nobler, P. (1998). Turn Around. How America's Top Cop Reversed the Crime Epidemic. New York: Random House.

Breton, P. (1966). L'informaticien et la sécurité: enquête sur un antagonisme. *Les Cahiers de la sécurité intérieure,* Entreprise et sécurité, 24:36-47.

Bulletin sur la sécurité de l'informatique. (1998). Sous-direction de la sécurité des technologies de l'information, GRC. Sécurité des TI. Janvier. No 45.

Campbell, F. (1997). High-Tech Advances Bring New Tools. *Police*, 21, 10:60-63.

Cansler, R. (1996). Technology Liability Considerations. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Cansler, R.E. (1998). Technology Liability Considerations. *The police Chief*, May:53-55.

Carpenter, G. (1984). Preliminary Considerations for the Impact of Microtechnology on Police Management. *Canadian Police College Journal*, 8, 2:93-106.

Carter, D.; Katz, A. (998). Computer Applications by International Organized Crime Groups. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Castells, M. (1996). *The Rise of the Network Society*. The Information Age: Economy, Society and Culture. Volume I. Great Britain; Blackwell.

Catalyst (1996). Denver Partnerships Produce Unexpected Evidence, 16, 2:1-2.

Clarke, R. (1993). Les technologies de la prévention situationnelle. *Les Cahiers de la sécurité intérieure*, 21:101-112.

Corsentino, D.; Pettinari, D. (1996). A Fork in the Road. *Sheriff,* March-April:1012, 35.

Coutorie, L. E. (1995). The Future of High-Technology Crime: A Parallel Delphi Study. *Journal of Criminal Justice*, 233, 1:13-27.

Dobeck, M. (1997). Taking Advantage of the Internet. *The Police Chief*, January:35-38.

Dorn, N. (1998). Du renseignement au partage des informations: l'intelligence protéiforme. *Les Cahiers de la sécurité intérieure*, 34:91-108.

Ericson, R.; Haggerty, K. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.

France, Ministère de l'Intérieur (1999). Assises de la formation et de la recherche dans la police nationale

(1999). Table ronde no 2: former à l'utilisation des technologies nouvelles. Paris: La Villette.

Fulton, R. (1995). When Law Enforcement Met Industry, Transferring Military Technology. *Law Enforcement Technology*, September:56-60.

Galland, J.P. (1996). Eléments pour une prospective de la sécurité. *Les cahiers de la sécurité intérieure*, 24, Deuxième trimestre:85-102.

Goodman, M.D. (1997). Working the Net. Exploiting Technology to Increase Community Involvement and Enhance Service Delivery. *The Police Chief*, August:45-53.

Grabosky, P. ; Smith, R.; Wright, P. (1996). Crime and Telecommunications. Trends and Issues. *Crime and Criminal Justice*, 59: .

Green Mazerolle, L.; Haas, R. (1998). 'The problem Solver'. The Development of Information Technology to Support Problem-Oriented Policing. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Haley, K.; Taylor, R. (1998). Police Stations in Cyberspace: A Content Analysis of Law Enforcement Agency Home Pages. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Hutchison, J.; Mays, J.; Moriarty, L. (1998). Teaching Statistics in the 21st Century: Technology in the Classroom. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Johnson, R. (1997). High-Tech Help. Robots Lend a Hand in the Labs. *Pony Express*, December: 18-19.

Kerr, J. (1999a). Inside the Web. Intranet Pilot Project Keeps the Force Connected. *Pony Express*, January-February: 7.

Kerr, J. (1999b). Making Connections, Computer Database Helps Investigators Piece Organized Crime Networks Together. *Pony Express*, January-February:16.

LeBeuf, M.E. (1998). Redefining Police-Community Relationships. Ottawa: Research Centre. Canadian Police College.

LeBeuf, M. E. (1999). Police de proximité et contrats locaux de sécurité- Que retenir du modèle canadien de police communautaire? Rapport présenté à l'Institut des Hautes Etudes de la Securité Intérieure-IHESI. Janvier.

Lingerfelt, J. (1996). Technology as a Force Multiplier. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Loree, D. (1987). Technological Innovation and Social Control: Some Implications for Police. *Canadian Police College Journal*, 11, 1:13-33.

MacDonald, V.; Martin, M.(1986). Specialists and the Personnel Structures of Canadian Police Forces. *Canadian Police College Journal*, 10, 3:189-226.

Manning, P. (1992). Technological and Material Resource Issues. In L. T. Hoover (ed.) *Police Management Issues & Perspectives.*

Martin, S. (1996). *The Impact of Information Technology Upon the Traditional Hierarchical Structures in Highly Bureaucratic Organizations*. Command College Class XXI. Peace Officer Standards and Training. Sacramento, California.

Marx, G. (1997). The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology. In P. Drogue (ed.) *Intelligent Environments*. Elsevier Science.

Marx, G. (1998). An Ethics For The New Surveillance. Page web consultée le 1998-10-2.

McLean-Lipinski, J.R. (1999). Enhancing the Use of Tehcnology in Law Enforcement. Page web consultée le 1999-05-06.

Mercier, P. (1998). On-Line Crime: In Pursuit of Cyber Thieves. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Moore, R.H. (1995). Technology and Private Security; What Does the Future Hold? Journal of Security Administration,.18,2:1-9.

Moriarty, L.; Dover, T. (1998). The Centralized Data Entry (CDE) System: One County's Attempt at Managing Burdensome Paperwork with Innovative Technology. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Morrison, R. (1996). Information Technology 2000. What's Ahead in the 21st Century. *Law Enforcement Technology*, June:40-43.

Myers, L.; Myers, L. (1998). Integrating Computers in the Classroom: A National Survey of Criminal Jusitice Educators. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

National Institute of Justice (1994). *25 Years of Criminal Justice Research*. National Institute of Justice. December.

National Institute of Justice (1997). *Technology for Community Policing*. Conference Report. Sponsored by National Institute of Justice, Office of Community Oriented Policing Services, National Institute of Justice. June.

Naulleau, D. (1998). Le bogue de l'an 2000: un révélateur de la vulnérabilité de nos libertés. *Les Cahiers de la sécurité intérieure*, 34:69-90.

Nogala, D. (1993). Le rôle de la technologie dans la police de demain. *Les cahiers de la sécurité intérieure*, 14, août-octobre:137-158.

O'Shea, T. (1998). Analyzing Police Department Data: How and How Well Police Officers and POlice Departments Manage the Data They Collect. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Ocqueteau, F.; Pottier, M.L. (1993). Vidéosurveillance et gestion de l'insécurité dans un centre commercial: les leçons de l'observation. *Les Cahiers de la sécurité intérieure, 21:60-74.*

Parsons, S. L. (1993). Technology Can Boost Safety in the Field. *Police and Security News*, 9,4:19-22,27.

Pilant, L. (1999) The Debate Over Encryption. *The Police Chief*, LXVI, 1:31-35.

Pilant, L. (1994). Spotlight on High-Tech Training. *The Police Chief*, July: 25, 27-33.

Pitcher, P. (1995). *Artist, Crafstmen and Technocrats: the Dreams, Realities and Illusions of Leadership.* Toronto: Stoddart.

Preimsberger, D. (1996). Cops and Space Scientist:New Crime-Fighting Partners. *The Police Chief*, October:108-114.

Public Inquiry Commission Appointed to Inquire into the Surete du Quebec (1999). Report of the Public Inquiry Commission Appointed to Inquire into the Surete du Quebec. Vol. 1, 2. Summary and Recommendations. Québec: Les Publications du Québec.

Quirion, S.; Lamy, O. (1999) La télédétection appliquée aux cultures agricoles et illicites. Sommets, 13, 2:22.

Rodriguez, M. (1995). An Overview of Law Enforcement Technology. *The Police Chief*, April: 15-29.

Rosé, P. (1996). L'informaticien et la sécurité de l'entreprise. *Les cahiers de la sécurité intérieure*, 24: 25-35.

Seaskaste, Inc. (1998). *The Evolution and Development of Police Technology*. A technical Report prepared for The National Committee on Criminal Justice Technology. National Institute of Justice.

Sheptycki, J. (1998). Reflections on the Transnationalization of Policing; the Case of the RCMP and Serial

Killers. *International Journal of the Sociology of Law*, 26:17-34.

Sloan, R.C. (1997). How Can Technology Help Police Be More Effective in Community Policing? In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Smietan, I.; Ferris, D. (1996). Detecting Concealed Weapons. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Soullière, N. (1999). Police et technologies: un bilan historique, un regard contemporain. Ottawa: Collège canadien de police, Centre de recherche.

Strandberg, K. (1998). Websites For Law Enforcement. *Law Enforcement Technology*, January:59-60.

Tafoya, W. (1997). Policing High Tech Crime. *Crime & Justice*, October, 23.

Wells, J.; Minor, K. (1998). Criminal Justice Students' Attitudes Toward Distance Learning as a Function of Demographics. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Wilsker, I. (1997). Cops on the Web. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.