REPORT ON VULNERABILITY

by
Dr. Jake V. Th. Knoppers

Working Group Sovereignty Aspects
Interdepartmental Task Force
on Transborder Data Flows

Department of Communications
Ottawa, September, 1982

TABLE OF CONTENTS

A. INTRODUCTION

1. BACKGROUND

The appearance in 1979 of a report by a Swedish government committee on "The Vulnerability of the Computerized Society"1/ served to focus debate on the effect of expanding and more intense application of computer-communications technology in society and the increasing electronic linkages, interdependencies and vulnerabilities of advanced industrial countries. Networks of interconnected computer systems are playing an increasingly important role in military, government and commercial environments. The quickening pace of the spread of computers, remote access terminals, advanced high speed digital links as well as ease of remote access linking facilities using a simple telephone let alone satellites will hasten the movement towards a wired society. Many developments and changes in modes of production, communication, provision of services and handling or manipulation of data and information have already reached a point of no return, i.e. a manual or mechanical non-electronic substitute is no longer possible. In addition, a substantial number of new economic activities have been started especially in the service sector, which could not exist without the support of computer-communications.

The introduction and spread of computer-communication technologies, has made possible cost-efficiencies, flexibilities and new opportunities in the production of and delivery of goods and services, existing and new by business as well as government. On the whole, the effects of the information revolution have been positive as were those of the earlier agricultural and industrial revolutions. Like its predecessors, the information revolution marks both a structural change and order of magnitude change in cooperation, linkages and interdependencies. But unlike its predecessors, the information revolution not only involves a basic change in mode and means of production and types of products, but it is also just as much a transportation revolution. It, therefore, impacts not only on the linkages and interdependencies within a society but also

accelerates in a very noticable fashion linkages and interdependencies between societies. The information revolution has already advanced so far in a number of areas that it has become extremely difficult to distinguish between domestic and international aspects of issues and concerns.

The importance of these developments is that

a. it will become increasingly difficult in a number of areas to discern between vulnerability issues of a domestic and a transborder nature;
b. a number of vulnerability issues of a domestic nature will have added to them transborder components of various degree of importance; and
c. vulnerabilities which arise in other countries can easily become concerns for Canada, as they are easily transmitted via computer-communication.

Insofar, as the nation-state has a responsibility for the well-being of its citizens (corporate and natural), it must know what the impact and possible affects of these developments are and might be. While there is considerable debate on the rapidity and intensiveness of the movement towards a wired society, there is no longer any doubt that developments have reached the point where impacts are being felt and the need to take action or not to take action becomes a decision making problem (both general and specific) of some urgency. These developments are fueled by two equally powerful forces working in tandem, namely, data processing capability (computing, i.e. the production process) and data transmission ability (communication, i.e. the transportation facility). Not only does advancing telecommunications technology provide for more efficient and sophisticated networks within a country, they also are used to link nation-states together in the same fashion. The combination of the movement towards a wired society with more and more international linkages has raised questions about the impacts and effects (both real and speculative). These concerns have found an expression in the term "transborder data flows".

A number of governments have already enacted legislation or introduced regulations either alone or in concert (Council of Europe, OECD) related to transborder data flows (TBDF) at present focusing on personal information.2/ Consequently, the Canadian government finds itself with the dual challenge of beginning a process of domestic response to the impact of integrated and expanding computer-communications as well as developing a policy strategy for responding to the actions of other governments as each of them reacts to the advent of the "Global Village".

As a first step, the Minister of Communications established, on 26 February 1981, an Interdepartmental Task Force to study the implications of rapidly increasing transborder data flows for the Canadian economy and for Canada's sovereignty. The Task Force's Steering Committee established three Working Groups, with respective responsibility for the analysis of the economic impacts of TBDF, the sovereignty impacts and the international environment.

Apart from addressing general issues and concerns related to transborder data flows, each of the Working Groups identified specific areas which would benefit from a more detailed and intensive examination and warrant the preparation of individual reports3/. One such set of concerns which relate closely to sovereignty impacts are those categorized as "vulnerability issues".

In the context of this report, vulnerability is considered to be "the likelihood of society being injured as a consequence of the increasing and more widespread use of computers and telecommunications", i.e. the possible impact of misuse or disturbances of computer-communications systems. In particular the focus of this study is to identify those vulnerability concerns where the transborder data flow factor adds a significant additional or new dimension.

2. PURPOSE AND STRUCTURE

This report, like those of the other Task Force project reports, attempts to address a certain set of TBDF concerns by concentrating on a specific and related set of issues. Like the other reports, it sets TBDF in a wider context. While the overall concept here may be that of the "vulnerability of the computerized society", the focus throughout is specifically on TBDF. Yet as with the other Task Force projects reports, considerable space is allocated to the current state of the art and the domestic scene. This is a necessary exercise since it should clarify the relative importance of TBDF to the domestic situation as well as identify whether a problem or issue is a TBDF concern or more properly a domestic concern with a TBDF aspect (of varying importance).

The basic goal of the report is to provide a factual assessment of vulnerability issues of specific concern to Canada. However, the subject of "vulnerability issues" being rather complex, the concerns wide-reaching, the difficulty especially for Canada in distinguishing between domestic and transborder computer/communications-based vulnerabilities, the lack of any detailed studies on vulnerability as such, as well as the context of rapidly evolving and changing technology, are all factors which make this task a rather difficult one. In addition, the level and context in which these vulnerability concerns are being addressed, i.e. this report, does not do justice to the increasing importance of the issues involved.

Several nations have, however, undertaken major efforts in evaluating vulnerabilities associated with the increasing spread and reliance on computer-communications technologies. They are Sweden, the U.S.A. and Great Britain, all countries with which Canada shares many common characteristics. Consequently, our discussions will benefit from noting the findings of these vulnerability studies. This is done in Part I of the Report.

Each of these major national studies was undertaken in a certain geo-policital situation, point in time and specific focus or context. But there are other vulnerability issues and concerns which are being

addressed in the context of transborder data flow discussions not addressed in these studies. Part I is, therefore, also based on available literature, reports that characterize the current state of the art, including both the state of technology and of current systems as well as oral and written contributions of government and industry participants4/.

The purpose of Part II is to identify and focus on those vulnerability issues which have a very strong transborder data flow component. Having identified these, Part II also includes an analysis and factual assessment of these vulnerability issues in the Canadian context and identifies concerns which could be considered unique to Canada. The concluding chapter of the report summarizes the findings of the project team and identifies possible direction for future work.

Finally, it should be noted that the question of possible "vulnerabilities" primary economic or cultural in nature have been addressed in other studies by the Task Force.

3. DEFINITIONS

One immediate difficulty was the question of definition of the term "vulnerability" which is a state of susceptibility to injury. It is a concept which has traditionally been qualitive in nature and only recently has the quantitative aspect been introduced. Vulnerability is dependent on two key aspects, the value of the assets to be protected as well as expectancy of loss and probability of occurrence. The latter two are extremely difficult, if not impossible to predict with a significant degree of accuracy.5/ In the TBDF context, quite often only the worst possible case scenarios have so far been highlighted and public concern is thus aroused.

Two basic problems present themselves here. The first is that in the real world, vulnerability factors (both physical and in terms of sensitive information) are not neatly organized into well-ordered sets of increasing sensitivity. The major difficulty lies in establishing criteria and

defining and identifying what are significant anticipated threats or hazards. The second problem arises from the fact that it becomes increasingly difficult to measure vulnerability as the links increase, i.e. as one moves from a tangible physical entity such as a computer installation or application to a computer system on to a communications network, then on to data/information flows and finally to the nation-state as a whole.

Although in theory, the solution to the threat or vulnerability problem is to assign probabilities to each magnitude of loss, in practice this is often impossible. Not only can some losses not be quantified but for many threats there is simply not enough regularity of occurence for "probability" to be meaningful. An obvious example is the vulnerability of a country's computer-communications network to terrorism. Major examples are:

- increased and more widespread reliance on computer-communications systems
- security of data flows
- computer crime
- use of satellites, i.e. remote sensing
- dependence on offshore data processing and expertise
- increasing importance of vital national information systems and information as a resource.

Other vulnerabilities can include such items such as business interruption factors which are important but which may be difficult to quantify and which vary from business to business. The question of "vulnerability" of computer-communications and increased reliance on the advancing new technologies and linkages in the context of TBDF is one where the past provides very little guidance, i.e., the area of low-incidence, high-loss risk analysis.6/

This is not to say that a study on vulnerability issues and TBDF is an exercise in futility and speculation. The report does identify a number

of substantial concerns which warrant attention because of their present and/or growing importance to Canada and increasing public concern. In many instances, there are however, no easy answers or solutions nor clear (natural) courses of action to follow.

The question of the ability to keep data confidential, i.e., to prevent unauthorized access or data flows, forms an integral part of vulnerability concerns. Unfortunately, the transborder data flow debate suffers from the fact that no distinctions are made between the different types of data flows and the appropriate levels of confidentiality (with appropriate security measures) that need to be maintained. The Report on Data Retention and Data Storage suggest a classification approach which would assist distinguishing between various levels of confidentiality, access and sharing of data and thus data flows.

It should be noted that freedom of information legislation in effect in a number of countries and the federal government's own Access to Information legislation (Bill C-43) makes a distinction between mandatory exemptions for information (defined as not disclosable if the information falls in a certain category and therefore requires protection) and discretionary exemptions for information which may be disclosed depending on the outcome of an injury balancing test. Of interest here, is the fact that U.S. freedom of information legislation defines oil industry related data as being vital to the national interest and therefore exempt from their freedom of information legislation.

In the context of the Canadian Access to Information legislation, the passage of such legislation and the resulting workings of it will increase the awareness of both government and industry as to what information requires protection from disclosure. The need to keep certain information confidential is shared by government, industry and individuals. However, each of these has a different set of confidentiality needs and concerns.

4. LIMITATIONS

The report is based on available literature, reports that characterize the current state of the art, including both the state of technology and state of current systems and networks. Not only is the concept of vulnerability at this level difficult to pin down but the (recent) past provides very little quantitative and hard information by which to evaluate the (up till now rather isolated) cases involving threats or vulnerabilities of computer-communication systems. On the other hand, the cases that have occurred do raise serious and valid vulnerability concerns. And, it may just take one single case of fraudulent use of computer-communications to warrant taking appropriate measures to reduce vulnerabilities, e.g. as was the case in the petroleum industry.7/

It should be stressed that this report is not to intended to be nor purports to be an in-depth study of vulnerability issues arising from "the computerized society" and it should be noted the discussion of vulnerabilities (and TBDF) as such is still in a rather primitive stage. It may be that in particular areas an appendix or footnote provides some detailed background information but the general vulnerability issues addressed in Part I are there primarily because in discussions in other countries or in the international context they form part of the transborder data flow debate. As will be seen later, for a number of these vulnerability issues, transborder data flows have little or no impact in adding to or reducing such vulnerabilities. For others, a transborder data flow impact exists but only as an important secondary or tertiary component of larger domestic concerns.

PART I - GENERAL VULNERABILITY ISSUES

B. ROLE OF NATIONAL BOUNDARIES

One of the major factors underlying the whole question of transborder data flows can be found in the fact that the developments in the convergence of computer-communications and especially the advances in communications technology are resulting in more cost-effective, integrated and "friendlier" networking systems not only within a country but between countries as well. Not only is it possible to dial direct to an increasing number of countries, but more sophisticated data communication networks, i.e. packet switched networks8/ of different countries are in the process of being linked together to form integrated networks. One particular feature of these data communication networks is that they are becoming distance insensitive, i.e. the distance of the data communication is no longer the primary factor in the price paid for the telecommunication service. These technical and economic developments in computer-communications are of importance to the discussion of transborder data flow aspects of vulnerability issues because they effect the ability to distinguish between concerns which are more of a domestic nature and those where transborder data flows play a minor or major role. Consequently, the role and nature of national boundaries warrant some discussion.

Traditionally, national boundaries which mark the territorial limits of the state have also served as locations at which sovereignty was exercised. Movements of goods and people were controlled at the frontier or at the location where they first landed, i.e. ports. National boundaries thus served not only to mark the territorial limits but also to enforce national policies and practices with respect to the movement of physical goods and persons. From a vulnerability point of view, the national boundary marked the limits of the entity to be protected with the boundary marking both the conceptual and physical line of defense, i.e. the concept of "secure borders".

Recent advances in interconnection of the physical electronic networks within a country and between countries have led to the development of electronic information networks whose functional boundaries more often than not are quite different than those of the political boundaries. Actually, electronic information networks act as, what geographers call, "functional economic areas". Relevant examples of functional economic areas would be the area from which a large city draws all its daily commuters or all the points served by an airline or trucking company. It is quite common for such functional economic areas to overlap several as well as differing political jurisdictions. Until recently, the legal framework, domestic as well as international, has been able to adjust and adapt to new and different functional economic areas as they apply to the movement of persons or physical goods; and the nation-state has maintained its ability to monitor and control such flows of goods if and when desired. Mechanisms used to maintain a national boundary include customs and immigration, landing rights, import or export restrictions, tariffs, etc. Measures to reduce vulnerabilities include the establishment and maintenance of armed forces, intelligence surveillance and law inforcement agencies as well as custom houses, visas, probihitions on import or exports, etc. To date in the area of electronic communications, "physical boundaries" that do exist are basically those that have been imposed on the carriers and communication networks not on the flow or content. They are maintained through various international agreements and revenue sharing settlements. Examples are the telegram, telex and telephone communication networks.

The convergence of computer-communications with the computer serving as the base of a time-sharing network often acting as a communication switch coupled with the introduction of distance insensitive pricing, has led to the creation of numerous functional electronic information networks with boundaries of their own. For example, a computer time-sharing system that can be accessed from different parts of the world has its "boundaries" extended by every new location from which a remote terminal is used. The result is that, for all practial purposes, in computer-communications physical national boundaries have little or no relevance to an increasing

number of computer-communication network users. A consequence of the computer-communication revolution is thus the disappearance of national frontiers in a functional sense and the fact that in an increasing number of areas, it is becoming difficult to distinguish between domestic and international vulnerability concerns. In addition, vulnerabilities which are introduced in computer-communication systems in other countries are now readily transportable to Canada via these networks.

C. COMPUTER SECURITY

As the information revolution is based on advancing and converging computer-communication technologies, it is not surprising that the first set of vulnerability concerns focused on the reliability of computer systems and the ability to protect systems, data and services from accidental and deliberate threats to confidentiality, integrity or availability.

Security is largely a negative attribute. It is difficult to demonstrate its presence. Insofar as security is the concept of minimizing loss and protecting vital assets (processing, transmission and data), i.e. reducing vulnerabilities, the discussion which follows talks in terms of security, unauthorized access, penetration, compromise, threats, etc.

Apart from physical security of the installation and in the context of computer-communications, security is really the prevention of four main problems,

- disruption or denial of use of computer system or the communication network, (i.e. reliability and availability);
- unauthorized access to information or release of information (i.e. confidentiality and privacy);
- unauthorized modification, manipulation;
- and or destruction of data or software programs.9/

Prevention against accidental errors are every bit as important, maybe even more so. In the context of this report, stand-alone computer installations i.e. those that do not allow remote access, can by definition not be accessed from outside of Canada and thus do not present a transborder computer security concern.

Reducing the vulnerability of computer systems is the responsibility of the organizations which operate the systems. The vulnerability of computer systems is therefore not a transborder data flow issue as such.

However, discussions of transborder data flow concerns both domestically and internationally, continue to include computer system security, or vice-versa. The transborder data flow question in relation to computer security is one of "Does the fact that one can attempt to access a computer system directly from outside of one's country, increase significantly (a qualitative-quantitative judgement) the vulnerability of our computer system"? For example, the introduction of direct long-distance dialing between two countries adds a significant number of possible remote access points. Does this constitute simply a numeric increase in possibilities of unauthorized access or also an increase in probabilities? Or, are there more individuals or organizations in that other country who may judge the data to be of value to the extend of being willing to attempt to gain access to it illegitimately? Can one utilize the same measures that one uses to reduce domestic vulnerabilities to reduce transborder vulnerabilities? etc.

Even though computer and communication technologies are converging, it remains useful to distinguish between vulnerabilities at the computer system and terminal level and communication network level. Accordingly, this section, while recognizing the constant interplay between computers and communications and the fact that in a number of areas the functions are so integrated as to be virtually indistinguishable, is divided into two major parts, one on computers and terminals (remote) and the other on communications.

One of the major vulnerabilities related to computer security is the lack of awareness of vulnerability of most computer systems to misuse and the mistaken belief that advanced technology will make the problems that do exist disappear. This is major point made by individuals as well as the Swedish and the U.S. studies.10/

Experience has shown that most of the existing systems can be (and frequently have been) successfully "broken" with less than three person-months of effort. This is true even for these systems to which serious security "repair" efforts have been applied. The system as a

whole may be secure but the question of whether the operating system itself is secure is often avoided. The state-of-the-art is such that security is not yet a mandatory feature of hardware, firmware and software available in the market place. Conversely, there is little pressure from customers for security, mainly due to customer confusion as to what is available, what could be available, what is needed and what they want. Further, users of computers do not in practice care very much about security, demand security or are willing to pay for its costs. This attitude seems to be changing as more highly integrated networks and data bases come into widespread use and the use of computers becomes more vital to the organization involved. Customers tend to wait for the vendors while vendors are waiting for an indication of demand. This passive tendency on both sides tends to mark the general nature of the security problem because the more knowledgeable security users demand solutions for their unique problems. More often than not such solutions have no general applicability and hence they do not become a standard part of a product line.

Further, the computer security problem is exacerbated in part by a widespread belief that changing and advancing technology will make the problem go away. So far companies specializing in computer security equipment or software have found sales disappointingly slow. The interest in and concern about computer security is building up slowly; the trigger consisting of a number of well-publicized and not-publicized (grapevine) instances of compromise of computer systems. Indicative of this growing awareness, is the marked increase in attendance at and frequency of conferences and seminars on computer security and the recent offering of specialized "computer crime insurance".11/

A number of recent developments in the computer areas are creating new risks in breaches of security and heightened awareness of a growing computer vulnerability problem. The main developments are:

- the introduction and spread of low-cost microcomputers (personal and small business) which by the mid-1980's could well number over

5 million in North America alone. Already more than 10% of these have communication capabilities. For an increasing number of new microcomputer products, communication capabilities are built-in. The microcomputer has also reduced the cost of a data line wiretap fraud from $50,000 to near $1,000; 12/

- the growing switch of user demand to remote compution services and a decrease in batch over-the-counter data processing. In 1965, batch held a 9:1 ratio over interactive processing. By 1985, the ratio is expected to be reversed.13/;

- the rapidly increasing quantity of computerized data stored and transmitted over communication networks;

- the trend towards linking a large number of computer systems together to be used for diverse applications by many persons at different locations which poses system design and management security problems that are orders of magnitude larger than those found in the design of previous generation of information systems. In addition, such systems are deliberately designed to distribute access, to make it easier for individuals to use the system and to decentralize administrative control of data processing. Consequently, security becomes more difficult both because of the increased numbers of persons who have access to computers as well as the factor of geographical dispersion;

- the increasing trend to user-friendly computer systems without a corresponding review of the adequacy of security measures;

- the soaring number of students and others acquiring computer know-how; and,

- the large numbers of employees and others who can access computers.

Further, a computer-wise generation is emerging that views most computer security measures as no more formidable than locks on a car door. In a sense, a number of computer systems have been taken for joy rides. A highly publicized case with equally well publicized TBDF implications for Canada occurred in 1980 when teenagers at Manhattan's Dalton School allegedly used their classroom computer terminals to dial into Telenet and from there into Datapac successfully identifying themselves as authorized users to computer systems of Canadian companies allowing them to take control of the computer. While in this and in other systems penetrated no funds were diverted, data files were compromised and damaged.

To many individuals breaking computer-communication security systems, represents a challenge not to be ignored. Not hindered by conventions, innovative and willing to spend countless hours, they present a threat to which often even the sophisticated software designed to restrict access to computer files is not adequate.

The rapidly increasing move by businesses to distributed processing compounds the problem. The number of remote terminals has more than doubled in the past five years and most of these remote terminals can be used to get into the organization's computer files or those of others. Insofar as the computer systems of companies operate on an international basis, a transborder element is added.

There appears to be general agreement that these developments increase vulnerabilities. The Swedish report noted that the introduction of smaller, more powerful and cheaper computers would have a tendency to reduce vulnerability of computer systems but that these could also be a new source of vulnerability problems. The U.S. Office of Technology Assessment's Report added that security management was becoming more difficult not only because of the increased number of persons with direct access to the system but also because of the geographical dispersion of the organizations involved.

Some background information on methods for reducing the vulnerability of computer systems and for the data in a system are presented in Appendix A. Insofar as a computer system offers remote access there is a transborder data flow component. However, from a technical sense, in most cases there is little difference in attempting unauthorized access and use from within a country or from outside that country. (See appendix B for more details on such methods). The measures to reduce vulnerabilities are basically the same.

The transborder vulnerability aspect is found primarily in that of legal and other remedies that one has at one's disposal to prevent unauthorized access to a computer system or to prosecute for such "offences". Even if domestic laws of a country are changed to reduce vulnerabilities of computer systems by providing adequate remedies, the lack of an agreement of some sort with other countries, from which one can readily attempt unauthorized access and use of computer systmes, may well nullify much of the hoped for reduction in vulnerabilities that domestic law was to provide. A secondary transborder vulnerability aspect is that as the communication networks of countries are linked, the number of potential threats (e.g. individuals or organizations) increases in relation to the increase in the number of possible remote access points and computer-literate individuals.

D. COMMUNICATION NETWORKS

Multi-system networks provide the means by which large numbers of geographically dispersed users can share resources and communicate with each other in a convenient way. The growth of networks of computers and remote access to computers can therefore be seen as a natural progression in the trend to share and use resources more effectively and efficiently.

Computer communication systems are not inherently secure. By the very nature of the way in which they are designed and how they are designed to function, computer-communication systems are basically insecure. They are designed to maximize the use of available resources, not to be secure. All efforts to make such a system more secure tend to reduce resource availability and use below optimum levels. And, given a choice, system designers and communications carrier managers will tend to optimize resource availability and to minimize or ignore security considerations. (The same holds true for EDP managers.)

Telecommunication facilities have already proved to be very sensitive to the effects of natural disasters, -floods, earthquakes and the like. They also have proved to be vulnerable to terrorist attack and to disruption by union employee action (most notably in the Britain where action by the unionized government telecommunication agency and EDP staff played a major role in bringing down the last Labour government).

Both communication land links and satellite circuits have shown themselves to be susceptible to sunspots, cosmic ray showers, aerial storms and other electromagnetic disturbances. These phenomena and their disruptive effects upon international computer communications have received, thus far, little attention from either governmental bodies or researchers. One exception is Electromagnetic Pulse or EMP.

So far this has not been a pronounced probem (domestic or transborder) nor can the full social and economic consequences of a failure to deal forcefully with this class of vulnerability be estimated clearly at this

point. Criteria for identification and classification of such vulnerabilities need to be developed. However, it should be noted that as electronic (digitized) data flows become more intensive, extensive and pervasive, the risks associated with these vulnerabilities will increase and thus warrant closer inspection and more detailed attention.

Many network vulnerability issues are straightforward extensions of those in any multi-user, resources sharing local computer network. There are however a number of issues which are unique to the telecommunication network particularly with respect to the vulnerability of communication lines. This section describes the more important of these.

1. Liability of Common Carriers and Data Flows

The telephone network was designed basically for the transmission of voice messages between people. The obligation of the common carrier has been to assure that its facilities survived disasters or efforts to compromise those facilities (typically, theft of services).

The common carrier has had little practical responsibility, or liability, for protecting the content of messages passing between authorized users of its facilities against alteration by, or unauthorize disclosure to third parties. As a matter of fact the liability of the common carrier is essentially very much limited by the terms of the regulations covering the carriers. This was confirmed by a 1975 Supreme Court decision (5-4) in the case of B.G. Linton Construction Ltd. versus CNR (49023LD 548). The overall effect of this ruling severely limits the common carriers liability (if any) for content, accuracy or timeliness of transmission.

If there are problems with the network, it has been the user who notifies the carrier of problems in data accuracy and should the user wish to reduce vulnerability of errors in data transmission, to a very low threshold, the carriers offer communication links for that purpose, e.g. conditioned lines.

Where computer-driven electronic messages represent values such as those involving the transfer of funds, the vulnerability of loss due to content, accuracy and timeless are usually addressed by those involved. Until now, closed user groups such as SWIFT have settled among themselves liabilities or damages resulting from errors in accuracy or timeliness of data transmission without resort to the courts.

It does seem, however, that those using a data transmission network to provide services do have liabilities. A recent ruling by the United States District Court of Illinois held that a bank is liable for its failure to make a timely electronic fund transfer involved in an international business transaction. As a result, a Swiss bank was ordered to pay an Illinois company over $2.1 million in damages caused by its mishandling of $27,000 telexed wire transfer in 1973. Although, the decision is being appealed, it points out that private international law in torts can, so far, accomodate the question of liabilities. The decision also points out the need for reducing vulnerabilities through risk analysis. However, the error in this case lay in procedure and the terminal telex not in the data transmission.14/ Uncertainties do exist as to who would and can be held liable in cases where an error in data transmission leads to an incorrect fund transfer.

Communication networks are playing an ever increasing important role with noticeable increases in speed, volume and value of the data transmissions. Consequently, accuracy and dependability become vital concerns. Where multiple linked networks are involved as is the case in transborder data flows, vulnerabilities will be minimized insofar as one is able to determine whether errors in a data transmission are due to the network and, if so, which network in what country.

2. Routing of Data Flows

The route of a data transmission is not as straight forward as it would appear from the outside. Actually, the network is just that, a myriad of comparatively short links connected by switching points of various types. It is best envisaged as a very complex spiderweb of sorts. Messages do not always travel the most direct paths between two points. Rather, they are routed in a path determined by the nature of the network's uncommitted capacity at the time, the goal being to optimize the use and, therefore, the revenues, of that capacity. Insofar as national networks are being integrated more and more, it may happen that data sent from one point in a country to another point in that country may very well cross one or several borders or the same border several times. While this may lead to policy conficts, it does not necessarily lead to increased vulnerabilities.

At the level of an individual time-sharing computer system, transborder data flow issues arise from the use of such a system to provide electronic messaging and other services between domestic points using a computer-based in another country.15/ The fact is that a computer system must be able to provide messages to its users and vice-versa and allow users to communicate with each other. As a result, such systems offer communication capabilities in the form of electronic mail or store and forward, etc. Again while this raises transborder data flow policy questions, it is not a vulnerability concern. As a matter of fact, the existence of the added possibility of communicating domestically via a transborder flow of this nature may actually reduce vulnerability, i.e. no dependency on a single system, for the individual user. Such developments may, however, introduce a vulnerability to the degree that they affect the revenue base of the carriers.

The Swedish Vulnerability Report found that Sweden had a very high degree of dependency on international data transmission circuits which pass through several countries. Of particular concern was the fact that this exposed Sweden to two types of vulnerabilities in its

transborder data flows. First of all, it rendered Sweden vulnerable to countries exerting pressure by threatening to disrupt transmission between Sweden and third countries. The second set of vulnerabilities lay in the possibility that some the countries might be more vulnerable than others to attacks on their communication systems i.e. by radical or terrorist groups. It may be noted in this context, that the Dutch PTT has proposed arming its security personnel as a response to the changing nature or attacks on communication networks, i.e. from vandalism to sabotage. Further, during the past two years, terrorist attacks against computer and communication centers have occurred in a number of European countries, notably France, Italy and Spain.16/

Transborder data movements would be affected by incidents of this sort. Data in transit through a country would be as vulnerable as that moving point-to-point from or to the affected country. The increased use of satellites for data transmission reduce these types of vulnerabilities by

- making countries less dependent on terrestrial transborder transmission via third countries; and,

- using satellites to restore, on a temporary or permanent basis, disrupted transborder terrestrial communications.

However, satellite communications-based networks present their own set of vulnerability problems. While the provision of back-ups facilities (either transponders or another satellites) is a common procedure, recently concerns have been raised about the vulnerability communication networks in general and satellites in particular to electro-magnetic pulse or EMP.17/ In addition, non-terrestrial communications are more vulnerable to "eavesdropping" than terrestial networks.

3. Security and Confidentiality of Data Flows

While the previous section dealt with vulnerabilities of the communication network as a whole, this section will address certain characteristics of communication networks affecting security and confidentiality of the data or information flows themselves.

To assure maximum feasible use of computer-communication resources, the communication systems are designed to make them as accessible as possible. Similarly, the systems have been designed for ease of service which means that many of the vital points are exposed and provide for easy physical access.

If someone has physical access to a communications circuit in which data communications traffic is moving in the clear (that is, unencrypted) and can physically attach a data terminal or recording divice to that circuit that can accept and properly interpret the signalling protocol and character representation scheme in use, one can read and/or copy the information moving over the circuit. This intrusion can occur passively, i.e. both parties to the transmission will be unaware of what is occurring. The telephone industry presently only can detect a fluctuation in the electrical characteristics of the transmission circuit that falls out of rather broad limits and the method of detecting that fluctuation is quite primitive. Again, if the service attachment appears valid to the network it is treated as though it were valid.

Message interception (along with the introduction of altered or out-right spurious messages) is easiest close to the source or goal of the transmission path unless defensive measures are taken. Most microwave communication require a "line of sight" for eavesdropping or interception. Concerns have been raised about the interception of classified government communications by other countries. This is more a matter of national intelligence and security than transborder data flow. However, non-classified but sensitive data can similarly be intercepted. This is

true especially where microwave or satellites are utilized for data transmission by the private sector.

Where multiplexing and/or message concentration features have been introduced into the computer communications network, message content can still be intercepted but greater technological resources and funds are required to do so. Where traffic passes through one of the newer electronic local office switches it probably can be intercepted, but what must be done to provide security in this environment is not clear as yet. Since this electronic switch essentially is a computer itself, it is likely that its resources could be applied back selectively against message traffic to get at its content.

While these are basically domestic vulnerability issues, potential transborder data concerns should be noted. As the communication networks increasingly rely on sophisticated computers for switching and routing of data traffic, these computers, like any communicating computers, are themselves susceptable to attack. A recent case of a radical group in California which launched a sophisticated computer-based attack against the local telephone company with the purpose of crippling the system by causing the switching and control computers to malfunction raises a transborder data flow concern in that such attacks can be launched from outside one's country.18/

Initially, movement of computer-communications through micro-wave and satellite links appeared to reduce its in-transit vulnerability to compromise. However, growing use by private parties of receiver antennas and press source reprints of amateur radio operator interception of sensitive messages moving over such links suggest that this type of computer-communication can be readily compromised if no defensive measures are taken.

Rendering data flows less vulnerable to interception is made possible through the use of a variety of technologies which in almost all cases rely on some form of scambling or encryption of the message to be

communicated. Any information transmitted can be regarded as sensitive if the leakage of it to unintended parties is perceived to be injurious to the transmitting and/or receiving parties. Within this definition, sensitive information ranges from scrambled pay-TV signals to oil well-head exploration data.

Almost all methods of protecting communications involve some form of scrambling or encryption.19/ Since World War II and especially in the last decade, the enormous progress in mathematics and digital technology have made it possible for the development of, for all practical purposes, foolproof and reliable encryption devices designed to protect information as it is transmitted through a variety of communication facilities. Public knowledge of encryption techniques was very limited until about 10 years ago. As a matter of fact, the U.S. intelligence and defence community is somewhat ill at ease with the development in recent years of the study of cryptology as a valid area of research. Those working in information theory and certain areas of operational research and mathematics are working towards the discovery of unbreakable algorithms as a scientific challenge. Consequently, the development of new and unbreakable algorithms is no longer restricted to national agencies (i.e, defence, intelligence, communication authorities). Research into new encryption schemes by academic and corporate scientists outside of governments, poses some difficult vulnerability questions, e.g. "What is the balance to be struck between the right of unrestricted enquiry in encryption research and the potential losses to national security and intelligence?" The publication of research results might encourage foreign countries and corporations to create new and unbreakable codes thereby cutting off not only code-breaking activities by intelligence agencies but also law enforcement, i.e., in the context of a legal wire tap or the interception and opening of the mails. On the other hand, if these new developments are kept from the private sector, might national security and well-being not be threatened as economic intelligence and data transmissions are becoming a more and more vital part of the workings of business? The private sector would want to reduce the vulnerability to

eavesdropping of data, electronic mail, electronic funds and commodity and other information transferred electronically.

In terms of advances in encryption techniques, two major items are worthy of note, namely, the establishment by the U.S. National Bureau of Standards of a Data Encryption Standard (DES) and new or recent research into techniques based on the "Public-Key" approach. (They are described in detail in Appendix C). The strength in any communication system lies in the protection of the encryption keys. Key control is therefore the vital element in reducing vulnerabilities of computer-communications which are encrypted.

From a transborder point of view a number of issues have been raised in relation to encryption of data flows. First of all, some have argued that a nation should develop its own encryption algorithms, otherwise, one is dependent on off-shore sources, e.g., the export of DES-based products is subject to the U.S. Export Arms Control Act. Further, there is a continual debate on whether encryption codes have hidden "trap doors" allowing the original developer to quickly break the encryption code used. However, national intelligence and security agencies develop and use their own encryption methods while for commercial purposes, encryption products on the market seem to offer sufficient protection in relation to the sensitivity of the data involved.

Second, transborder data flow issues arise from conflicts in national policies and regulations regarding the use of encryption in data transmissions. For example, in West Germany the use of coded or encrypted messages are not permitted by the Bundespost. In some states, such as France and Great Britain, the question of registration of encryption codes used in transborder flows of private or commercial data is being raised. Connected to this issue are concerns about requirements for disclosure of data transmissions even for data which is simply passing through a particular country en route to a further destination in another country. So far, these concerns have not become a significant issue but they could quickly become so as they are related to the ability to exercise

sovereignty and enforce laws. Currently, regulations do exist on the flow of certain hard copy material via the mails, e.g. obscene or hate material. Should these principles be applied to electronic data transmissions, enforcement might require the registration of encryption codes. This could well have an impact on the need for confidentialty of data flows by the private sector.

A rapidly emerging TBDF issue is the encrypting or scrambling of broadcast or video signals transmitted via satellite whose footprint covers others than the originating nation especially where someone in another country decodes and sells the data. At present, this issue has arisen primarily in the context of broadcasting (e.g. Home Box Office) but as encryption is being used more for sensitive data the same problems could arise in other areas, e.g. videotex and teletext, as well as transmission of any other data.

4. Computer Crime

Based on the assumption that data in a computer-communication system or use of the system is of value or can be manipulated to create a value, the level of vulnerability is a combination of the worth of these values to the owner and the ease or probability with which these values can be appropriated without authorization or adequate recompense. Such actions are commonly known as "computer crime". In the sense that the extensiveness and frequency of "computer crime" is an indicater of the degree of vulnerability, it warrants some discussion. First of all, it should be noted that this concept suffers from two weaknesses, namely,

- it assumes that computer crime exists and can be defined; and,

- it assumes that the definition of computer crime is uniform and that therefore computer crime can be measured.

In many countries, "computer crime" as such does not exist because it is not covered by the criminal code or like legislation. The definition of

computer crime is a decision that will vary from legislature to legislature depending on each's social judgement about what property rights (and other rights) the penal laws should enforce.

Statistics on computer crime vary widely. Some include all criminal acts where a computer is involved. But a distinction must be made between those cases where a computer is an instrument in the execution of an illegitimate or fraudulent act and where it itself or the data is the object of abuse. Much of the "computer crime" where the computer was one of the instruments in the carrying out of a recognized criminal act should not really be consided a "computer crime". The analogy would be, as one expert put it, "To classify a majority of the fraud cases as pen or pencil crimes".20/ Consequently, many of the statistics on computer crime are misleading. In addition, within organizations what constitutes computer abuse is not firmly established, i.e. "theft of computer time". Lack of adequate definition and data thus disguises the true picture of vulnerability and computer crime. Further, if a remote attack against a computer is successful because of some existing vulnerability, its vulnerability may persist and thus the attack is not publicized. Companies often do not report computer abuse because of fear of adverse reaction of customers or stockholders.

Very little hard estimates are available as to the possible exent of computer crime as well as future trends. This is because, as stated above, actions which one might consider to be computer crimes are not so by definition under national legislation; second, often the computer is merely one of the instruments used to execute a criminal act; third, the concept of "theft of computer service" is often not yet accepted in domestic law; fourth, many "crimes" are not reported and the same holds true for computer crimes; and finally, society's attitude in general is such that "most computer crime" is looked at more with some amusement than concern.

While statistics on computer crime remain suspect, the spectre of gigantic losses from computer crime has triggered the creation of a new breed of

casualty insurance. In the fall of 1981, Lloyd's of London began offering insurance to banks against computer-related theft and fraud. Its success has led to a number of other insurance companies (mainly in the U.S.) offering electronic and computer crime insurance, including non-financial companies even adding protection from accidential losses or damages arising from so-called computer pranks. Many companies who have availed themselves of this new type of insurance did so not because of the danger of the frequency of losses from computer crime but that when a loss occurs, it could be of major proportions and costs.

Most of the discussion of computer crime so far has focused on security without taking into account the possibility of international computer crime of various natures. The Swedes noted that criminal acts which constitute a serious threat are sabotage, espionage and terrorism. They also recognized that advances in the use of computers may give rise to crimes against property of entirely new dimensions and that data crimes do occur and have been extremely difficult to detect. The U.S. assessment noted that threats against computer systems appear on the increase and as society grows more information oriented, the risk of theft will increase along with the potential payoff for its success. Organized crime is also seen as a threat. In the context of transborder data flows, the concept of computer crime raised additional concerns since the perpetrator may be at a remote terminal in country A, manipulating the computer system in country B and then have the "stolen goods" transfered to country C. For national penalties for computer abuse to be affective and the vulnerabilities raised by transborder data flow minimized, will require international agreements on (a) the locus of the liability; (b) uniform or compatible definition of computer crime within each country; and (c) perhaps, a convention to bind countries to enact provisions making it illegal to use computer facilities in a foreign country via transborder telecommunications without having authorized or legal access to that computer in that foreign country.21/ It has been suggested that the work done in developing the legal framework to combat terrorism and airplane hijackings could serve as a model for applying similar legal instruments

to the protection of computer-communication systems involving transborder data flows.

5. Satellite Transmission

Satellite-based data communication networks offer reduced costs and vastly increased capacity for data flows. Such networks not only form an alternative to terrestrial-based networks but also open up many new transborder data flow possibilities. Considerable discussion is currently taking place in many countries on the role, management and use of these new transborder data flow facilities. One of the primary concerns is the possible effect satellites may have on the revenues of existing terrestrial networks. In a sense, the debate is similar to that faced by railways and ships more than two decades ago and their possible loss of long-haul passenger and cargo traffic to the airlines. In many countries, the debate in essence is analogous to asking whether railroad and trucking monopolies should also run the airline and airports and build the airplanes.

Aside from this debate, satellite transmissions have a wide footprint, which generally does not respect national boundaries. Attempts at unauthorized eavesdropping are therefore relatively simple to execute. On the other hand, satellites do offer high speed/volume point-to-point communications facilities allowing a country to be less vulnerable to different kinds of disruption of the kind that terrestrial transborder data flows passing through several countries may be subject to. Satellite-based point-to-point communications combined with reliable encryption and various switching mechanisms can reduce vulnerabilities of transborder data flows.

6. Remote Sensing satellites

Concerns have been raised about the possible vulnerabilities raised for a country due to remote sensing by satellite. The vulnerability is perceived (by some countries) as the "siphoning off or theft" by

multinationonals and industrialized countries of information of one's country's resources and possible state of wealth or poverty. There is also concern, about the vulnerabilities that may be created through the introduction of this new technological facility and capability for massive data collection activities about one's country over which one presently has no enforcement jurisdiction to safeguard sovereignty and vital interests. It is feared that vulnerabilities are introduced when one country has a marked technological advantage of access to such superior data collection, transmission and processing, this being easily translatable into a substantial economic advantages, i.e. advanced or sole knowledge about mineral deposits or possible agricultural crop yields.

It must be noted here that use of remote sensing satellites for national defense and military intelligence purposes are of a different order than those addressed by the Task Force. But it should also be noted that the advanced capabilities of such surveillance satellites as reported in the popular press, fuel general apprehension by the public and politicians about vulnerabilities introduced by remote sensing especially when one neither has access to the data or the ability to process it.

For the purpose of the Task Force, the major focus is presently on the LANSAT and the weather remote sensing satellite series, i.e. publically available or purchasable data. It can be argued quite convincingly that remote sensing satellites are reducing general vulnerabilities in that they are rapidly becoming invaluable for man's coping with nature, e.g. earthquake prediction, navigation, silviculture disease control, etc.

At present, the U.S. through NASA possesses the remote sensing satellites. NASA seems to have overcome many of the initial objections raised by the lesser developed countries about possible vulnerabilities due to "data drain" by adopting a policy of making the LANDSAT data available at a set and uniform price to all who wish to purchase it, i.e. countries as well as private industry. During the next few years, France plans to launch its SPOT satellite (1984), Europe an Earthnet satellite (1987) and Japan

similar marine and earth satellites so that in the near future other countries will be having their "own" remote sensing satellites.

Thus while transborder data flow concerns pertaining to remote sensing satellites and associated vulnerabilities will persist, often fueled by speculation in the popular press or by academics, it currently cannot be considered a transborder data flow vulnerability as such. To date, the data collected by non-military satellites is publically available at the same time to all who wish to purchase it as are the software and the hardware to process the data.

E. OTHER VULNERABILITIES

Thrown in with the discussion of transborder data flows are a number of vulnerability issues of a wider or different scope than computer-communications as such. These are reviewed in this chapter.

1. External Threats

The Swedish study on vulnerability issues related to the increased use of and dependencies on computer-communications was headed by the Minister of Defense. The report of the British Security Commission 21/ was the result of a study undertaken as a result of concern about the possibility of disclosure of sensitive information to Soviet Bloc intelligence services. To these discussions is added the concern that as the use of computer-communication systems becomes more pervasive and their uses more critical to economic and military functions, the state becomes more vulnerable to terrorist attacks on its computer-communication systems, attacks launched via transborder telecommunication facilities. Computer systems and the data they contain represent dense concentrations of value and are becoming targets for both domestic and international terrorist groups. Apart from technical and procedural controls at the system level, the reduction of vulnerabilities due to terrorists acts would benefit from international conventions dealing with criminal acts related to computer-communications in general, e.g. the approach taken to stop airplane hijacking.

a. Emergency Planning

One vulnerability arising from an external threat is that in time of war one must count on decreased use of computer-communications. The Swedish report stated that failures in emergency planning can have disastrous consequences if damage occurs in computer-communication systems and to data that are nationally important. The Report also noted that emergency planning for computer-communication systems was not what it should be. In both the government and civilian sectors,

there is a problem of contingency planning with specific focus on computer-communication dependencies.

Emergency planning as such is not a transborder problem. Emergency planning is the responsibility of the organization involved (government or private sector). Transborder data flow considerations do, however, arise if the contingency plans include the provision of a back-up computer centre or essential records (data) storage plan involving locations in another country.23/ A number of questions arise in this context

- to what degree are vulnerabilities increased or decreased by having these back-up facilities in another country? In this context, it may be noted that having an operational back-up contigency plan in the first place is usually the most significant aspect in reducing vulnerabilities. The question to be asked in the TBDF context is, "To what extent do companies and service bureaus rely on offshore entities for back-up facilities?" It has not been possible at this time to formulate a detailed answer to this important question.

- What are the legal or regulatory complications arising from the movement of data as part of the enactment of a contingency plan? It may be that the confidentiality of data or data subjects protected in one country is not the same as in the other country and vice-versa. Further, the question of government records retention, inspection, regulation, and other like requirements, i.e. "to maintain, books records, retention, inspection, regulation, and other like requirements, i.e. "to maintiain, books recordes, accounts, etc.", in light of off-shore back-up facilities raises another potential set of problems.24/

With respect to subsidiaries of multinationals there are two sides to the coin. On the one hand, the computing-communication requirements

of the subsidiary may be too great for the offshore parent to handle. On the other hand, it could be that the subsidiary forms part of a distributed data processing network in which case the data processing load could be shared by the other parts of the multinational system provided that communications would allow for this.

To date very little is known about contingency planning practice related specifically to computer-communications with back-up facilities, involving more than one country. (See also Appendix A.3) However, the last few years have seen the emergence of several companies specializing in offering complete computer-comunications back-up facilities and services. A number of factors favour having the back-up facilities close at hand. First of all it is already difficult to regenerate a computer-communications facility at a remote location. The further the back-up facility is away from the host data centre the greater the logistical problem of moving data, people and suppliers. For users with remote terminals or link-ups the closer one is to the host data centre the easier it is to establish back-up communication facilities. Yet it should also be noted that for many vital records programs, one of the main criteria is that the back-up data, i.e. copies of records, be kept at a location far away from the host site, at a location which is much less vulnerable to natural or man-made catastrophies.25/

b. Electromagnetic Pulse (EMP)

During the past year, the phenomena of electromagnetic pulse and its potential to severely disrupt computer-communication networks has received great interest. While it had already been noted that the use of nuclear weapons will lead to severe damage, if not total destruction, of specific computer-communication networks, i.e. in the explosion impact area, recent attention is focused on the possible use of nuclear weapons to knock-out all communication networks, electrical power grids and systems based on microchip technology over a radius as large as 2,000 kilometres or more. Electromagnetic pulse (EMP), is the name given to a very brief pulse of high voltage

that can be generated by certain types of nuclear explosions. By exploding such a weapon at a high altutude, the EMP created would swamp or burn out computer and communication equipment. Most vulnerable to EMP are computer circuits, transistors and silicon chips, i.e. all microelectronic-based products and services.26/ The more modern a nation's computer-communication infrastructure, the more susceptible it is to EMP.

Protection against EMP is probably not cost-effective except for the military where other criteria apply. Still the military does rely on the public telecommunication networks while the government does so to an even greater degree. In the U.S., Bell is taking some precautions. Some circuitry is being designed to reduce its ability to conduct EMP while in other areas especially vulnerable components are being insulated.

Designing new devices to be EMP-proof or EMP-hardened and their installation is expensive and from a risk-analyst's point of view probably not cost-effective in non-military applications.

Uncertainties exist about the effect of EMP on satellite communications. Concern about this is quite high in the U.S. because a substantial amount of its high-security communication is by satellite. Very little discussion has taken place as to the effect of EMP on the data itself, i.e. stored in electronic form.

While the use of modern technology has increased vulnerability to EMP, it has also provided a possible solution, i.e. fibre optics. Fibre optical devices and communication networks operate on pulses of light and thus are generally less vulnerable to EMP except where they rely on switches utilizing microelectronic chips. It is in this context that the Northeast Light Corridor Project of the U.S. linking a number of east coast cities using fibre optics takes on added significance.27/

Although the question of EMP is often raised in the context of transborder data flows, vulnerabilities due to EMP are more a domestic than a transborder concern. Insofar as domestic computer-communication networks are disabled, transborder data flow capabilities will be affected. But the relation of EMP to transborder data flows is only secondary. The vulnerability of computer-communications to EMP (and nuclear weapons in general) is a domestic political and military concern.

2. Personnel

In the report of the British Security Commission, Lord Diplock stated that the high demand for trained computer staff coupled with a comparatively rapid turnover of computer staff led him to conclude that from a security point of view, computer staff should be viewed as "birds of passage". While Lord Diplock's observation was directed at the civil service, both the Swedish and the U.S. reports also took particular notice of the key role that personnel plays in reducing or increasing vulnerabilities. The vulnerabilities related to personnel are two-fold.

First of all, the mobility of computer staff does mean that people with an intimate knowledge of the hardware and software of computers and the value of the data stored in that system as well as the measures taken to protect the system and the data are constantly leaving the organization. Quite often the organization does not review and adjust its security procedures after the loss of such key people. Vulnerabilities of this sort are basically an organizational or domestic concern. Transborder data flow related vulnerabilities enter the picture only if a country is dependent to a noticeable degree, on foreign skilled manpower. The Task Force Report on Skilled Manpower Shortages addresses in detail this set of concerns.

The second vulnerability concerns the degree of dependence on foreign maintenance expertise for one's computer-communication systems. The

Swedes noted that dependence of foreign maintenance expertise also increases vulnerability. SARK went on to note that systems engineers and programmers often build systems so complex that only they can manage or repair them. SARK therefore emphasized the need for good documentation as well as good labour-management relations to reduce vulnerabilities introduced through dependencies on key individuals. This is a common concern and not generally one of a transborder data flow nature.

However, the availability in recent years of remote on-line diagnostic and repair services introduce a new set of vulnerabilities with serious transborder data flow implications. In order to reduce maintenance costs, allocate key personnel skills more effectively and introduce a more cost- effective means for servicing increasingly large numbers of similar computer systems, various members of the computer industry have introduced remote service centres. These service centres are sites with concentrated skilled expertise and appropriate computer systems designed to monitor and diagnose problems of the computers of their customers via remote access or dial-in. Using remote on-line diagnostics, one can either guide on-site repair work or even execute the repairs by running the customer's computer from the remote service centre performing the required diagnostic tests. Service of this type can also involve the transfer of sensitive data from the customer's system to the computers of the remote service centers.

There are a number of transborder data flow concerns which arise from this development, all related to the possibility of such remote service centres being located in another country. First of all, an increasing number of systems are supported solely via remote on-line diagnostic and repair service centres. No longer are service engineers close at hand for a particular system. And should there be no remote service centres in a country, one is dependent on transborder expertise and service. Second, remote on-line diagnostics requires access to the (whole) computer system often

including the data as well. Quite apart from general computer security issues involved, there may be restrictions on access to the data that would be compromised if such remote on-line diagnostics were allowed. This is especially a factor for public institutions which must maintain confidentiality of data because of a law or regulation (whether in machine-readable or hard copy form).

Given the trend that skilled expertise is a scarce and increasingly costly resource, computers (systems and applications) are beginning to be mass-produced, i.e. especially minicomputers, and distributed in an increasing number of different locations, remote on-line diagnostics and repair services will become an increasingly attractive means for providing customer support.

However, transborder data flow concerns will require a careful assessment of the trade-off between reliable and cost-effective maintenance service from another country and increased dependency on foreign expertise on the one hand, and, the question of maintaining local control over access to data, on the other.

3. Concentration

a. Computer Systems

The Swedish Report reviewed that vulnerabilities are introduced by concentration of computers and computer networks. In its analysis, the Report distinguished between two types of concentration, functional and geographical. It defined functional concentration as large central systems or large service bureaux with centralized operations and many users (dispersed by type of use or geographically). The Report noted that a large number of functionally sensitive systems are computerized or being changed to automated systems, e.g. those for banking, trading, process control in production processes, traffic control, etc.

The U.S. study stated that the increasing reliance on functional automated systems for electronic fund transfers, cheque clearing houses of the banks, the stock exchange, commodities and future trading houses and similar activities of national importance "create concerns which the government will soon have to address".

Geographic concentration, i.e. the accumulation of computing capacity in certain specific areas, also introduces vulnerabilities. At the time the Swedes completed their initial Report, specific reference was made in this regard to the Stockholm area. Consequently, it recommended that an increasing spread or dispersement, both functionally and geographically, of computer systems would have a distinct advantage from the vulnerability point of view.

It should be noted that a number of years have passed since the Swedes made these findings. Of particular importance is the introduction of increasingly more powerful and less-expensive mini-computers, a trend that certainly does seem likely to continue for some time to come. Insofar as these powerful mini-computers (and even in some instances, microcomputers) make it feasible and cost-effective to carry out data processing on-site, vulnerabilities due to geographical concentration will be reduced. And where this leads to less reliance on off-shore data processing, transborder data flow related-vulnerabilities will be reduced. Unless geographical concentration involves reliance on off-shore data processing, this is not a transborder data flow vulnerability.

The situation is not as clear with respect to functional concentration as this is usually related to the offering of a particular type of computer-based service involving a common master data base, e.g. credit verification, information retrieval, financial transaction clearing systems. More often than not such applications are anchored at one (or a few) master system nodes since it is necessary for a user to have access to all the data. Where functional systems important to a country are located outside that country, a

transborder concern is introduced. Otherwise this remains a domestic vulnerability issue although the question of a remote attack on such a system from outside the country remains a transborder concern.

One of the major developments in the 1980's will be the appearance, on a commercial basis, of true distributed data base systems wherein the location of any particular item of information in the data base may be anywhere in a national or international network, in which access to the data is handled totally by the system and the system can continue to function even if a number of its components, i.e. a computer here or there, fails to function.

While such a development greatly decreases vulnerabilities associated with geographical and functional concentrations, it brings with it an accompanying reliance on communication networks and, where several countries are involved, transborder questions.

b. Data

Closely related to vulnerability questions raised by geographical and functional concentration of computer systems are concerns about concentration of data. A number of European countries had the unpleasant wartime experience of having registers of personal information fall into enemy hands. Because many of these countries are unitary states politically and assign mandatory personal indentity numbers, means that many different data banks are easily linkable and the various levels of government share information readily. Further, in many of these countries, the state occupies a very large role in society. It is therefore not surprising that the Swedish report found that many personal information registers contain information so sensitive as to be of interest from the vulnerability aspect. Of particular concern is the possibility of these "registers" falling into enemy hands and greatly assisting the enemy's war effort. Consequently, the Swedes felt that this might be reason to review plans as to which computer systems should be

destroyed or removed in a war situation. SARK also felt that certain data banks containing information on companies and detailed technical and geographical data should be included in this review. The situation described above is a domestic vulnerability question.

Privacy issues however, do have a strong transborder component. Concentration of data brings with it another set of vulnerabilities. Concentration provides a more clear focus for both attack as well as defense. Insofar as concentrations of data offer a more valuable target for unauthorized access or manipulation and this is possible via remote access, a certain element of transborder vulnerability exists.

4. Economic/Financial

While the Working Group on Economic Aspects addressed the question of economic impacts from the perspective of balance of trade, industrial strategy as well as an analysis of specific economic sectors, it would be worthwhile to note here some specific vulnerabilities economic or financial in nature which may arise as a result of converging technologies and transborder data flows that effect economic policy and the ability to regulate certain kinds of financial transactions.

The increased use of electronic fund transfers adds a certain degree of vulnerability to the nation's ability to exercise effective monetary policy. Electronic funds transfers (EFT) recognize that money is merely a form of information, the exchange of dollar bills being only a demonstration of ability to pay. Money as information resides in computer storage with payments consisting of digitized data transfers and transmissions between one machine and another. Further, there is some concern about the impact electronic fund transfers systems will have on the ability to monitor the effects of monetary policy. If funds can be transferred instantly from demand (chequing) accounts to savings accounts, and vice-versa, the

distinction between savings and transaction balances will become less relevant. In addition, the velocity of the nation's money supply may increase sharply and may become less predictable. A significant number of these electronic fund transfer systems are international in scope and operation. Since many of these electronic fund transfer systems are international in scope and operate with relatively few restrictions on the transfer of funds in and out of many countries, there are transborder data flow implications especially where large amounts of EFT can take place on a daily or even hourly basis speculating on either the trend in interest rates, foreign exchange value of currencies or both. The result may well be less certainty as to the effectiveness of domestic monetary policy and means for measuring and predicting the money supply and its velocity.

Another vulnerability concern is raised by the very real possibility of the establishment of off-shore trading houses. The world's first fully automated commodities exchange, called INTEX, is scheduled to open in Bermuda this fall. Dealing only in commodity contracts it allows its members to buy and sell on-line via a system which queues, executes and records these orders. INTEX is considered a forerunner of an off-shore stock exchange of a similar nature. The vulnerability and sovereignty concerns are that such systems allow one, via one's (personal) computer to buy and sell orders directly into the off-shore exchange, all outside national boundaries including those of the jurisdiction of the securities exchange commissions as well as those of the tax man. So far technical problems have proved to be the main barrier but, with the advent of linked packet switched networks, off-shore trade such as that offered by INTEX may become common place.

5. Information as a Resource and Vital Link

The discussion of the vulnerability of society in relation to transborder data flows is based on the assumption that we are moving from an industrial society towards an information - or knowledge -

based society and that flows of information within a nation and among nations act as the arteries of such a society. A better and clearer understanding of the role of data or information as a resource is and will remain a vital element to such understanding.28/ While the role of data or information is often explained using the analogue of resource extraction and manufacturing, it does have characteristics which require a new analytical framework. In the context of this Report, one should note that

- data is not depleted or consumed;
- more extensive use of data can increase its value;
- data can be combined with other data or information to provide other (new) products and services;
- converging computer-communication technologies make data or information processing or value-enhancing less location specific, i.e. in the sense that raw resources are geographically bound; etc.

It suffices to say that the role of information in an information-based society is not yet fully understood. However, there is sufficient evidence to show that the role of information, information systems and flows in society is becoming increasingly important. The nature of risk or vulnerability of society is being changed by much of the new computer- communications technologies on which modern society depends. The U.S. study found that because the new technologies can be designed to operate more reliably and efficently than the systems they replace, the risk that any particular mechanism may fail has been reduced. However, should an accidental or deliberate disruption accur, its cost can be much larger, even catastrophic. In addition, the more society becomes dependent on the reliable function of large, single integrated computer-based support systems or a limited number of such systems in key areas, the possibility of collapse of one or several of such systems could be disastrous. To the extent that such systems rely on transborder data flows for their effective functioning, the degree to which those

systems are linked to those in other countries and/or the degree to which one is dependent on the reliable functioning of such systems, in other countries, vulnerabilities of a transborder nature are introduced.

The Swedish Report found that the vulnerability due to increased reliance on computer-communications technology was "unacceptably high." The U.S. study stated that the "federal government has a responsibility, as yet undefined, for an increasing number of computer-communications systems which although owned and operated by the private sector are performing increasingly vital functions in society and are thus becoming fundamental to our well-being". The reason that these are becoming governmental concerns lies in the vulnerability of such systems and the fact that a major systems failure or compromise could cause significant harm to the economy of the nation or its citizens.

Of note, also is the increasing role information plays in decision-making processes of an economic, social, cultural or political nature. The heightened importance of international competition and trade coupled with decreasing availability of raw or basic resources are requiring both governments and industry to improve and speed up their decision-making capabilities. Computer-based information systems (public and private) are growing in importance for this purpose. This requires access to information with timeliness, accuracy, and exclusiveness being very important in determining the value of information. In the transborder data flow context, there exists a need to have access to information outside of one's country as well as the ability to filter, analyse and/or process such information once received or obtained. The converse also holds true.

The concern with these data flows is two-fold. The first concerns the problem of ensuring an "equitable trading" relationship with respect to the export of "vital" information resources. The concern

stems from the current uncertainty as to whether information is being exported as an unfinished product (or data) to the detriment of an indigeneous production/processing (read value-enhancing) industry. There is also a concern that information is being sold at a below-market value, i.e. not being able to process, distribute or market the end-products in one's country, one is forced to sell the information at (what later on turns out to be) an "unfair" price, e.g. licensing or royalty fees are too low. And finally, does the export of certain raw data flows once established hinder the establishment of a an indigenous information-based industry in that product/service line? The Report of the Economic Aspects Working Group provides an answer to these questions for some key sectors.

Further, there can exist a substantial number of industrial sectors where a country is dependent on importation of computer-based services which it has a latent capacity to produce. The question of such dependencies form part of transborder data flow debate and are often discussed in terms of vulnerabilities of a particular sector.

The second set of vulnerability concerns is related to the role of data/information flows as vital cogs in the delivery of goods and services. Advances in computer-communication technologies have had the effect of either radically transforming the delivery of existing services to such a degree that they would find it very difficult if not impossible to continue operations, or led to the introduction of new services which operate only in electronic mode. Operations which are very dependent on transborder flows include electronic funds transfers, airline reservations, hotel booking, brokerage services, banking services, car rentals, ship chartering, information retrieval service, etc. and soon even some of the new videotex (Telidon) based services.

Computer-communication data transmissions have also become essential to the proper functioning of multinational enterprises. Using common (networked) data bases, multinationals rely on TBDF to increase

productivity and to provide better planning coordination and control of financial, procurement, production, inventory, distribution and marketing activities. Consequently, as reliance on computer-communications becomes more widespread, vulnerability becomes a more important factor and as reliance as international data flows increae, transborder issues become a greater concern.

While debate and discussions on questions of increasing vulnerabilities associated with increased and more widespread use of computer- communications systems will undoubtly continue, it should be noted that the use of new technologies has greatly reduced other vulnerabilities (or uncertainties). However, while many of the new vulnerabilities raised by the computer-communication revolution are primarily matters of domestic concern, for an increasing number, transborder flow issues have become a significant component and can no longer be ignored.

PART II - THE CANADIAN CONTEXT

F. THE ROLE OF NATIONAL BOUNDARIES

The convergence of computer-communications and especially the advances in communications technology yielding more cost-effective, integrated and "friendlier" networking systems, are resulting in the disappearance of national boundaries in the electronic world. The fact that advancing computer-telecommunication are by their very nature becoming less distance sensitive and less terrestial-bound means that physical or territorial national boundaries will not necessarly translate into electronic national boundaries. As a result the maintenance of "electronic national boundaries" if needed will become an exercise increasingly depended on a conscious desire and political will. It is an area where the past or previous experience is of little help. In fact, it may be a hindrance or even have a negative effect if the conventions and habits covering the physical world and physical goods are extended to the digitized world or even those of the "electronic highways" to that of the "electronic ocean". Further, there is a great deal of doubt whether any attempt at establishing an "electronic boundary" for data in the classical sense, i.e., via a customs or toll both, is feasible especially now that voice (human communications) are also being digitized.

The introduction of direct long-distance dialling of distance insensitive pricing and linked packed switched networks have led to the creation of a North-American domestic communication network resulting in the virtual disappearance of the U.S.-Canada boundary as far as the user is concerned. Current arrangements involving TCTS and CNCP through interconnection agreements with the U.S. domestic carriers via Telesat are such that Canada-U.S. terrestial transborder traffic is treated as a simple extension of Canadian and U.S. domestic services resulting in a fully integrated and highly efficient North American telecommunication network. As a result, Canadian domestic vulnerability concerns are intricably linked with the question of transborder data flows.

The situation is somewhat different for "overseas" data flows which are handled via Teleglobe through switching centres or gateways in Montreal, Toronto and Vancouver. Here again, the trend is towards providing more efficient, higher volume and speedier data flow capabilities which will make the crossing of national boundaries more and more transparent to the user as time goes on. The introduction of direct-distance dialling on many routes as well as the establishment of interconnect links between data communication networks indicates a growing disappearance of national boundaries for Canada in the functioning of computer-communication networks. The question of the role of Telesat, Teleglobe as well as private commercial carriers in satellite transmissions is currently under discussion, the main emphasis being on the search for equitable and workable formulas for revenue sharing.

G. COMPUTER SECURITY

The Report of the British Security Commission found that "the use of computers in the public service for the storage and retrieval of classified information is the area of physical security which causes the Security Commission the greatest disquiet". While the Commission was impressed by the thoroughness of the physical security taken to deny authorized access to computer installations and disks and tapes upon which information is stored and also to prevent the use of terminals by unauthorized persons, it did not feel qualified to express an informed view as to whether such installations are entirely free from other forms of vulnerabilities.

It should be noted that the complexity and diversity of the systems being introduced into the work-place places severe strains on the specialists required to develop and maintain them in production environments. The shortage of specialists and the pace with which the technology is advancing results in the individual specialist being required to spend all their energy in simply making systems operate effectively. The resources required to analyse security concerns, which are themselves as complex and diverse as the machines to which they apply, can often not be justified. This leads to a requirement for the generation of standards to simplify the specialist efforts in applying appropriate safeguards, so that adequate, and cost-effective security can be selected.

The Canadian Government has put considerable emphasis on this area, and is providing a comprehensive set of standards which can be selected and applied dependent upon the type of system in use and the sensitivity of the information being processed. Eventually eight chapters of detailed standards will exist, covering security considerations in the following areas, as they apply to computers: Administrative and Organization, Personnel, Physical and Environmental, Systems, Hardware, Software, Operations and Communications. The first three chapters have already been published. From a transborder data flow perspective, the key chapters are the latter four. Work on these is in progress with all expected to be

published by the end of 1983.29/ In the interim, information on proposed standards is being provided to departments of the Federal Government by the RCMP's Security Evaluation and Inspection Teams, who provide a centralized consulting and inspection service for computer security concerns in the Government.30/

While certain bodies of the federal government such as the Security Advisory Committee (SAC), the Interdepartmental Computer Security Panel (ICSP), the Communications-Electronic Security Committee (CSC), the EDP Evaluation and Inspection Team (SEIT), etc., are responsible for various aspects of computer/ communications security within the federal government and with government contractors, no mechanisms or criteria currently exists for assessing at the national level either the vulnerabilities of increasingly important vital domestic computer-communication systems and their international linkages or the increasing importance of non-classified but nevertheless valuable or sensitive data.

Domestic as well as transborder data flow concerns (and speculations) will continue to be raised about the security of such systems. This requires the establishment of criteria for the identification of both systems and data of vital national interest and an assessment of the role of transborder data flows in increasing or decreasing vulnerabilities. At present lack of awareness of potential computer security issues seems to be the greatest vulnerability. Further, it is becoming increasingly difficult to distinguish between computer and communication security issues. The trend in computer use towards remote access, linked systems and distributed processing makes communication capability and integrity a vital element in the functioning of computer systems. In communications, increasing use is being made of computers not only as switching devices but adding other data manipulation possibilities as well.

H. COMMUNICATION NETWORKS

1. Liability of Communication Carriers and Data Flows

Mention was made in Chapter D.1 to the 1975 Supreme Court decision in the case of B.G. Linton Construction Ltd. versus CNR and the electronic fund transfer case involving the Swiss Bank. The emphasis in both cases was on the timeliness of the execution of the transmission. In both cases the content of the message was delivered correctly, the lack of timeliness being the prime cause for court action. The question of liabilities that may acrue to a common carrier due to errors in the data transmission itself has not yet been addressed in Canadian Courts.31/ While concerns continue to be raised in the domestic as well as transborder context about data flows going astray (e.g. packets), resulting in serious loss, no serious incidents have yet occurred.

2. Routing of Data Flows

It has already been noted that terrestial telecommunications with the U.S. are treated as an extension of the domestic network via Telesat while other transborder data flows both terrestial and non-terrestial are handled via Teleglobe. The introduction of satellite-based communication systems offer reduced costs and vastly increased capacity for data flows. While Canada has a very strong capacity in the use of satellites for communication purposes, it is faced with the decision of how to approach the question of licensing the use of commercial satellites for transborder data flows, i.e. the development of a new operating environment for transborder data flows. One factor which must be noted here is the strong move towards deregulation in the U.S. both in terms of allowing "domestic carriers" to provide international services and the resale by companies of excess capacity of their internal communication facilities.

The vulnerability question here is more one of an economic nature. The introduction of many and diverse new ways for transmitting data including the use of cellular radio and cable indicates a trend towards what in transportation terminology is called "multi-modal transport". Insofar as national communication networks are being integrated more and more, and linked with those of other countries, the routing of data flows can well take on the characteristics of a multi-modal transportation system.

Its geographic position and advanced telecommunication capabilities make Canada less vulnerable or dependent on terrestial transborder data transmission via third countries than might be the case of Sweden or other countries. Canada has direct links both terrestial and non- terrestial with those countries it engages in the vast majority of its data flows.

3. Security and Confidentiality of Data Flows

As an advanced industrial society making extensive use of computer-communication networks, concerns about security and confidentiality of data flows are similar in Canada as in other countries. The fact that Canada-U.S. data flows utilize a common technical support infrastructure make it difficult to distinguish between domestic and transborder vulnerabilities.

The debate on research in encryption in the private academic sectors which is quite strong in the U.S. has only found a muted response in Canada. Presently, publically-funded research on encryption is being carried out at Queens University under a major strategic research grant from the National Science and Engineering Research Council (NSERC).

The need to take active measures to ensure confidentiality of data flows is recognized in certain sectors of private industry, i.e. financial institutions and the oil industry. Questions of

registration of encryption codes or requirements for disclosure of data transmission has not arisen. Concerns have been raised, however, in connection with the scrambling of various kinds of broadcast transborder flows emanating from satellite transmissions.

The question of security and confidentiality of data flows through the use of encryption and other means could quickly become an transborder issue since it is directly related to the ability to exercise sovereignty and enforce laws. Policies of other countries will impact on the ability of Canadian persons and companies to maintain desired confidentiality of data flows. Another set of issues to be resolved in this context is the rapid convergence towards similar data transmission systems originating from different backgrounds, i.e. the question of "electronic mail" and "store and forward" capabilities of communicating computers and international conventions for postal services and telecommunications or the use of videotex via cable, telephone or broadcast links.

4. Computer Crime

As in other countries, Canadian statistics on computer crime and abuse are sparse and speculations are often extravagent. No one knows how large the problem is. The proliferation of microcomputers and distributed processing is increasing the potential for abuse. Microcomputers may also foster a new security threat, one that arises from the growth of public data bases which can be accessed through personal computers. Authorized users might abuse their right of access to the data by copying, repackaging and then selling it. But microcomputers can also serve to prevent computer abuse through monitoring who has access to data or for encryption purposes. As more management and decision-making information is computerized, particularly in high-technology, financial and resource related companies, such strategic data will become the targets of competing companies and foreign governments. Further, many people mistakenly put a heavy emphasis on site security whereas for communicating

computers emphasis on system and data security offers better protection against computer abuse.

Assessing risk of computer crime or abuse in the absence of crime probability statistics is difficult. The fact that current Canadian law does not recognize unauthorized copying as theft while the case of R v. McLaughlin (1980) 2 S.C.R.33 has made it clear that there currently are no penal consequences attached to the unauthorized operation of a computer as such.

While a long-range program is underway at the Department of Justice looking at the "property" aspects of data, proposals have been made to amend the Criminal Code to provide some immediate relief. These proposals would make it an offense to fraudently or without authority use a computer or any part of the related access network right back to the terminal as well as making it an act of mischief for persons to, without authorization, damage or alter data or information stored in a computer.32/

The enactment of penal consequences for "computer crime" will reduce domestic vulnerabilities. But since Canada's computer-communication networks are integrated with those of other countries, especially the U.S., the transborder vulnerability arising from persons enacting what would be considered a computer crime in Canada from outside of Canada via remote access will remain until such time as international conventions reduce this vulnerability.

5. Satellite Transmissions

Specific vulnerabilities of an economic or cultural nature introduced by satellite transmission are being addressed in other reports of the Task Force. While countries such as Columbia have laid claim to orbital parking spaces directly overhead its sovereign territory, i.e. locations for geosynchronous satellites, the technical possibility of placing satellites closer together in space coupled

with Canada presently having surplus satellite transmission capacity due to foresight and planning, mean that for the present and immediate future Canada will not be dependent on others for satellite transmission and vulnerabilities of this nature have thus been minimized.

The strong trend towards deregulation of the whole telecommunication industry in the U.S. has placed a strong impetus on the need to define the role, jurisdictions and policies for satellite-based transborder data both public and private flow services. Many Canadian branch plants of U.S.-based MNE's would benefit from participation in company wide international satellite-based point-to-point networks. This would increase TBDF both in volume of data as well as more cost-effective intra-company data flows related to transaction, control, operational and management information functions. The question of how to maximize the benefits of new technology in this context while minimizing possible vulnerabilities is a problem that has yet to be resolved.

6. Remote Sensing Satellites

Canada has two earth stations capable of receiving and analysing LANDSAT data. Canadian capability for interpretation and analysis of remote sensing data (i.e. that which is publically available) is one of the most advanced in the world with the fastest turn-around time. As a matter, of fact Canada has become one of the major exporters of LANDSAT earth stations.

Canada is currently reliant on foreign (U.S.) satellites for data and does not plan to launch its own remote sensing satellite, RADARSAT, until 1990.

As a general practice, remote sensing data on Canada is received only, NASA turning the LANDSAT transmissions "on and off". Current Canadian policy is to inform other countries if they are being

observed and to make such remote sensing data available to them. Often other countries, i.e. the U.S. and Denmark, request Canada, to make and process LANDSAT observations of some particular area of their country. In the private sector, the oil and gas industry are the biggest purchasers of remote sensing data in Canada followed by the forest industry.

Current arrangements for data access and use are arrived at through government to government negotiations. Recent U.S. policy emphasis on cost-recovery had led to dramatic price increases for access to LANDSAT data. As long as the U.S. pursues this cost-recovery policy to its logical conclusion, this is placing increased pressure on the privatization of the LANDSAT program. In that case the Canadian government would be dealing with a private corporation.

While remote sensing remains a vulnerability concern in the transborder data flow debate, Canada has minimized possible vulnerabilities in this area by creating a viable and technologically advanced indigeneous capability. At the same time, the policies followed by Canada in its use and sharing of remote sensing data and technology as well as its policy of notifying third party countries when they are being "observed" would seem to answer positively many of the transborder vulnerability concerns raised in the context of remote sensing related issues.

I. OTHER VULNERABILITIES

As a nation increasingly dependent on a computer-communication infrastructure, Canada shares most of the vulnerabilities identified by the Swedish, British and U.S. studies. So far Canada has been spared foreign terrorist attacks on its computer communication systems. Determining whether such a threat exist and taking adequate countermeasures is presently the responsibility of the RCMP.

a. Emergency Planning

In the context of transborder data flows and emergency planning, the question is "What is the degree of reliance on off-shore information flows and data processing capacity in times of local or national disasters and emergencies". In the event of a nuclear attack, Emergency Planning Canada is responsible for ensuring the continuance of government. On the macro-level, the nuclear war (doomsday) scenario, Emergency Planning finds it not prudent to rely on computer-communications. Responsibility for identifying and ensuring in peace and war of computerized data necessary to operate, rests with each government department, with the Department of Communications having an overall concern in this area. With respect to coping with peacetime disasters, the government's Emergency Planning order identifies particular ministries as having certain emergency peacetime responsibilities. Although to date no thorough survey has been carried out, there is little indication that government agencies would be relying on off-shore data flows or data processing capabilities in times of emergencies. Specific attention has not been paid to the private sector.

While emergency planning as such is not a transborder problem, the lack of an analysis or study of contingency planning for vital national computer-communication systems (public and private) makes any evaluation premature as well as any statement on the degree to

which transborder data flow vulnerabilities that may arise due to off-shore data processing or data flows suddenly cut-off.

In the private sector, there has been an notable increase in Canadian companies offering full contingency planning or back-up facilities. Canadian companies do store back-up data outside of Canada and also rely on off-shore data processing facilities and services for back-up. It is not possible at this time to make any statement as to whether, apart from legal complications that may occur, such transborder arrangements increase or decrease vulnerabilities. The lack of specific attention being paid to the role of vital computer-communication systems as such at various levels of emergencies (peacetime or wartime) also hinders our evaluation. Vital national information systems that need protection or contigency arrangements, whether in war or peace have not been sufficiently studied. No specific ministry is currently being charged with this task although the Minister of Communications does have the peacetime emergency responsibility to "control, regulate and maintain all essential telecommunications." However, public concerns continue to mount fuelled by media reports on the black lining to the silver cloud of high technology. But more important, many operations vital to the functioning of society have become automated to the extent that the point of no return to manual systems has passed. Criteria for identifying vital national information systems and ensuring that adequate protective measures and contingency plans do exist is rapidly becoming one issue that must be addressed.

b. Electromagnetic Pulse (EMP)

The vulnerability of Canada's computer-communication systems to EMP is basically the same as that of similar advanced industrial societies. Canada's vast geography and the fact that communication links play a very vital role may add an added vulnerability concern. The dangers of EMP are receiving attention by both the government and the common carriers. Protection against EMP is more a domestic

vulnerability concern than a transborder question even though EMP will probably continue to surface in the context of transborder data flow discussions.

2. Personnel

The Task Force Report on Skilled Manpower Supply and Constraints noted that Canada like other highly industrialized countries also faces a shortage of computer personnel, and it is therefore unlikely that Canada will be able to reduce this shortage by importing such skills from abroad. The Report also found that Canada may lose highly qualified people to the U.S. Further, the Report quotes the CADAPSO brief to the Parliamentary Task Force noting that the U.S. turnover rate in 1979 of 38% was much higher than in Canada. The Report discusses possible measures for reducing the skilled manpower shortage and in that sense answers a particular set of vulnerability issues related to computer personnel.

The question of remote on-line diagnostics represents a new set of vulnerability concerns for Canada. In the first place almost all of the main frame and mini-computers installed in Canada are imported with the highest proportion of imports coming from the U.S. Further, as the communication networks of Canada and the U.S. basically function as a domestic network, U.S. manufacturers can readily service the Canadian market from their remote service centres in the U.S. A particular problem is added where remote on-line diagnostics become the standard means for providing (quick) service for a particular series of computer systems.

An example which made the news in 1981 concerned Burroughs Corporation's Remote Support Centres and the computers of the Canadian Employment and Immigration Commission (CEIC). These computers suffered a malfunction and Burroughs desired to dial into CEIC's computer systems (which utilize Burrough's computers) from a Remote Support Centre in the U.S. The Unemployment Insurance Act as

well as Part IV of the Canadian Human Rights Act restrict access to CEIC data to authorized officers only. In this case, it would not have mattered if the remote service centre was located in Canada or outside of the country. The fact that at present most of the remote service centres are located outside of Canada will tend to place issues concerning remote on-line diagnostic and repair services in the transborder data flow arena. Whether or not the introduction of remote on-line diagnostic and repair services reduce vulnerabilities of computer systems by offering a complete (often 24 hour) trouble shooting service versus the fact that it presently increases off-shore dependencies and possible compromise of data confidentiality is a question which requires further and more in-depth analysis before one can venture a more definitive evaluation. From a technical point of view, measures can be taken to reduce or negate the possibility of access to data in a computer system which is being serviced on-line. The development of standards or guidelines to this effect, would reduce the vulnerability of access to sensitive data while at the same time allowing for on-line diagnostic and repair.

3. Concentration - Computers and Data (Personal)

Like many other countries, the computer systems in the 1960's and 1970's in Canada were characterized by concentrations of data processing in Montreal, Ottawa, Toronto and Vancouver. Since then geographical concentrations can be found in the provincial capitals as well as in Saskatoon, Calgary, London, Kitchener-Waterloo to name a few. The trend towards using stand-alone minicomputers and distributed data processing is also working towards mitigating vulnerabilities due to geographical concentration.

It should be noted, however, that while data processing services are being geographically dispersed both in the open market sector, i.e. service bureaux adding service centres in different locations to service those areas, and the closed market sector, i.e. the spread of distributed processing and local minicomputers, the same dispersement

might not take place for interactive computer-based information retrieval and transaction services, i.e. I.P. Sharp, the Canadian Institute for Scientific and Technical Information (CISTI) or the Bank of Montreal will probably continue to service their customers from one functional central data base.

Here again these are more domestic than transborder concerns. However, the Task Force Report on Public On-Line Information Retrieval Services does indicate a high degree of dependency on off-shore information services which are functionally concentrated.

During the past few years, both the public and the private sectors have developed sensitive functionally concentrated systems in such areas as some government personal data banks (e.g. SIN, UIC, CPP, medical records, etc.), banking, airline reservation and insurance services, corporate management systems, etc. Not being a unitary state, like many in Europe, jurisdiction is shared in Canada. This has the effect of dispersement of government data banks both geographically and in extensiveness and detail of contents. Nor does Canada have a system of mandatory assignment of personal identity numbers. As such Canadian vulnerabilities in this area tend to be less severe than those of their European counterparts. Besides most of these vulnerabilities are of a domestic nature.

However, various provincial commissions reporting on the confidentiality of personal information reported that extensive and intensive concentrations of data banks on Canadians were being maintained by foreign-owned companies often outside of Canada. While privacy is not being addressed at this time by the Task Force, it is and will remain a major vulnerability concern. The recent Parliamentary discussions on new Access to Information and Privacy legislation (Bill C-43) made this quite clear. Legislation has already been or will be enacted at the provincial level and will soon be enacted at the federal level on access to information and the protection of personal information. The enactment of this legislation will have a

strong transborder impact both in terms of the development of overall TBDF-privacy policies in harmony with domestic legislation as well as forcing a review of practical technical operational considerations of data storage location and data flow/data sharing. Such a review would bring to light specific transborder data flow practices and vulnerabilities especially, if and when, privacy protection is ever extended, in some form, to the private sector.

4. Economic/Financial

The Report of the Economic Aspects Working Group is addressing the question of economic impacts and vulnerabilities from the perspective of balance of trade, dependence on off-shore data processing as well as an analysis of specific economic subsectors. The vulnerabilities identified in chapter E.4. apply equally to Canada as an advanced industrial country. The problem of coping with the technical ability to electronically transfer funds in very large quantities, or the execution of transborder financial transactions by individuals directly from their home both within Canada also pose new challenges for policymakers. The increasing ability to execute financial, stock and like transactions outside Canada's national boundaries and the question of jurisdiction of security exchange and regulatory commissions coupled with the fact that facilities for this purpose are becoming commercial realities introduces a new set of vulnerabilities. The rapidly disappearing distinction between demand and interest-bearing accounts (leading to the disappearance of the former) coupled with transborder electronic fund transfer also pose a challenge to the control of monetary policy e.g. through means for measuring and predicting the money supply and its velocity.

5. Information as a Vital Resource and Links

A clearer and better understanding of the role of data or information is vital to coping with the information revolution as is the establishment of criteria for identifying of "national information

systems" which serve as the main underpinnings of the information society. Their disruption or loss of data integrity would harm national interests and, insofar, as they could be subject to remote attack the element of transborder vulnerability is introduced. It is not the within the scope of this report to identify such vital national information system or establish criteria although such a process would greatly assist the discussion on vulnerabilities (domestic and transborder). However it may be useful to note that the U.S. study used the following criteria for "vital national information systems",

- substantially national in geographic scope
- substantial national interest involved
- organized by government or private organizations or groups to collect, store, manipulate, and disseminate information about persons or institutions
- based in some significant manner on computers and related information and communication technology.

U.S. examples include FEDWIRE (an electronic funds transfer network operated by the Federal Reserve System), nation-wide computer-based credit card and check authorization services (e.g. VISA, American Express, Mastercard, Telecheck, Telecredit), nation-wide electronic mail services operated by several private firms and the U.S. Postal Service, computerized air traffic control systems, airline reservation systems of major air carriers (e.g. United, TWA, American), the computerized automatic quotation system for obtaining over-the-counter stock prices operated by the National Association of Securities Dealers, interconnected networks of personal computers such as MicroNet or the Source, etc.

The discussion on information systems as vital links and possible associated vulnerabilities will not progress until such systems are identified and their susceptability to disruption analyzed including

the degree to which the transborder element adds or reduces vulnerabilities.

With respect to data itself, a well-established program exists in government for reducing the vulnerability of unauthorized or accidental disclosure of classified data. Likewise programs do exist in most major organizations (public and private) for vital or essential records although their application to machine readable records is undergoing further development. What is not being addressed is the question of what is meant by "sensitive" non-classified data. The enactment of access to information and privacy legislation by different levels of government will assist in identifying "sensitive" data in the public sector. However, much of the transborder debate over sensitive data focusses on the private sector, i.e. the whole concept of information as a resource.

Apart from providing a summary review of the vulnerability question and the transborder context, the debate (or clarification) cannot progress much further until an acceptable working definition is given to "vital national information systems" and the question of "sensitive" but not classified information in the public as well as private sector is addressed.

J. CONCLUDING SUMMARY

The convergence of computers and communications technologies is making it increasingly difficult to distinguish between vulnerability or security concerns of each. The introduction of new networking capabilities and the trend towards linking national communication networks between nations so that national boundaries have become functionally transparent to the user are blurring distinctions between domestic and transborder concerns. The increasing dependence of society on computer-communications and data stored in electronic form means that disruptions in the functioning of such systems or loss of integrity of the data will have increasingly wider impacts. While on the whole the benefits of these transformation have been positive they also carry with them certain risks or vulnerabilities. How to minimize the vulnerabilities while maximizing the benefits of computer-communications technologies is a challenged faced by the public and private sectors alike.

The review of some of the major vulnerability issues in this report should be viewed only as an initial step. The fact that in the electronic world, national boundaries have increasingly less relevance in the use of computer-communication systems means that for many domestic vulnerability concerns the transborder aspects cannot be ignored.

Some of these general concerns are found in the area of computer security and it may be noted that for every threat, a technical countermeasure can be found. But the greatest vulnerability seems to be a single lack of awareness for the need of computer security. In this sense, the best counter-measure to vulnerability is to inform and advise and to raise the level of consciousness and knowledge about security and vulnerability. Within the Canadian government, a number of agencies are charged with ensuring that an appropriate levels of security and protection are instituted for governments systems and data is classified where necessary while others are

charged with ensuring the integrity of communication systems. Insofar as these measures ensure against unauthorized remote access, transborder vulnerabilities are reduced. What systems are vital and what data "sensitive" has not yet been fully examined, and no means presently exists to address the question of "sensitive" but not classified data especially in the private sector.

Presently no penal consequences are attached to fraudulent use or abuse of computer systems and data. No reliable data on computer crime exists in part because of lack of definition and legal recognition. A few isolated incidents do show that computer-communication systems are more vulnerable than is generally thought. The emergence of computer crime insurance, in its own right, does indicate a recognition by the private sector of the vulnerabilities and associated risks involved in misuse of computer systems. Changes to the Criminal Code have been announced to provide some immediate relief. However, given the state and trend of computer-communications technology, which allows attacks to be made on computer systems and data from outside Canada, a combination of domestic and international effort is required to effectively reduce vulnerability to attacks using transborder data flow facilities.

The convergence of computers and telecommunications is leading to a point where security of computer systems and data communication systems must be viewed as a common issue. This is especially true in the context of transborder data flow concerns. Future discussions and analysis will be well served by addressing computer and communications security, i.e., vulnerability issues, as a single set of concerns. They can no longer be kept separate.

The new data communication technologies reduce old vulnerabilities and introduce new ones. Many of the vulnerability concerns raised extend beyond the mere technical aspects. As a matter of fact,since technology often offers many options, the question becomes more one of seeking a constructive direction or route which minimizes

vulnerabilities. More and more, such decisions will require an integrated approach with due recognition of the transborder element where appropriate.

Much has been written on the question of vulnerability of society, transborder data flows and other issues arising from the impact of advancing computer-communications technologies. In reviewing the literature and the debates over the past few years, it seems that the discussion has not really advanced except where new problems are being added. However, public and parliamentary concerns and uncertainties continue to grow. The establishment of this Task Force, and other like groups before it, indicate the need for a continuing response mechanism. So far the responses of government have been ad-hoc.

The concern about increased dependencies on computer-communications and vital national information systems calls for an ongoing dialogue between the government, the private sector and the public as does the question of what is meant by "vital" or "sensitive" data. To date no such dialogue exists although the same information issues are being addressed simultaneously elsewhere, e.g. the discussions on videotex touch on many of the same issues. There thus seems to be a need for some mechanism for addressing these information issues on an on-going and integrated basis. Sweden and the U.S. present two types of examples for doing so.

The assessment of transborder data flow issues in this Report suffers from the lack of an available assessment of domestic vulnerabilities. As the use of computer-communication technologies increase, the debate will intensify while the concerns become more widespread. Ad-hoc responses, e.g. a Task Force, will not only become increasingly inefficient because of the need to develop an understanding of a wide range of interrelated information issues, they also require a response time which may be too long.

Most of the vulnerability issues addressed in this report are primarily domestic in nature even though the transborder data flow concerns add an important and sometime new element which cannot be and must not be ignored. While the initial focus of vulnerability issues was on technical issues, this is no longer the case. Just as there is a need for an on-going dialogue between the public and private sectors, there also exists a need to look at the wider vulnerability concerns and to treat these information issues as part of an integrated whole (even if for analytical purposes one may separate the components).

While a number of nations have studied, to varying degree, various aspects of vulnerability issues of the "computerized society" and transborder data flows, only Sweden so far has taken the step of establishing an on-going response mechanism and action plan, thereby moving from the study and general discussion stage to taking some concrete and practical steps. 32/ On the one hand, Canada's advanced telecommunication technology and computer capacity make it less vulnerable in a number of transborder areas which are of great concern to other countries, e.g. satellite transmission and remote sensing. On the other hand, that same advanced technology has led to the integration of the Canadian domestic network with that of the U.S. This has heightened the awareness of the increasing difficulty in distinguishing between domestic and transborder information concerns well as the recognition that in order to adequately address domestic information issues arising from computer-communications issues, the transborder data flow element will become an increasingly important factor which must be addressed.

As stated in the introduction, this report does not pretend to be nor is it intended to be an in-depth review of vulnerability issues arising from the "Computerized Society". It has focused only on those vulnerability issues which continue to form part of the ongoing debate on transborder data flow questions. If it has clarified these issues and given some sense of awareness and direction, it will have met its objective.

Footnotes:

1. "The Vulnerability of the Computerized Society: Considerations and proposals", Report by a Swedish Government Committee, Stockholm 1979. (This is a summary English translation by John Hogg of a Swedish government report published December 1979 and titled "ADB och sämhallets särbarhet, övervägaden och förslag". The Report is the result of the work of the "Committee on the Vulnerability of Computer Systems (SARK)" established on 26 May, 1977 by the Ministry of Defense at the request of the Swedish government).

2. See Report of the International Aspects Working Group for an overview of privacy considerations and actions by other countries and international organizations.

3. See Appendix ??? of the Task Force Report for the list of the reports of the Task Force.

4. See Appendix ??? of the Task Force Report for the list of participants.

5. In practical terms, risk analysis is the method whereby an organization identifies assets and values associated with them and specifies particular threats or vulnerabiities and evaluates the countermeasures to these by calculating the expected cost arising from these threats before and after applying the countermeasures. The reduction in the expected cost or loss provides the yardstick against which one judges the worth of the countermeasures. Risk in the context of risk analysis can thus be defined as the sum of expected losses over a certain period of time, e.g. a year, as the result of undesirable events with expected loss being the dollar loss of an event or threat multiplied by the probability of the loss occuring in a given year.

6. However, this is not a severe limitation provided that reasonable estimates are utilized in performing the risk assessement calculation. In some applications high/low estimates may be utilized to determine the expected range of risk under the worst case versus best case or ideal conditions. The average of the best and worst case loss expectancies can be used as an approximation of the actual real world loss expectancy that is likely to occur for a given category of loss. A possible injury or vulnerability test involves a number of factors. The first is that of specificity, i.e. the possible injury must be precise not merely a vague general vulnerability. The second factor is that the possible injury must be substantive, i.e. clearly identifiable with a "known" effect or impact so that the cost of the precautionary measures will outweigh those of the injury. The third factor is currency, i.e. the possibility of the identifiable vulnerability or threat must be one that is real in the present or in the foreseeable future. It may very well be that successful attacks which occurred in the past are no longer current threats either because adequate countermeasures have been taken or the technology involved has changed and may even no longer be in use. And, finally, the fourth factor is that of probability (already discussed), i.e. there must be a reasonable likelihood of the injury occurring, not merely a hypothetical possibility.

Risk analysis to determine future policies needed because of increasing dependence on automated computer-communication systems require low-incidence, high-loss risk analysis. This is a new area and no one has really developed a way to do it while present risk analysis techniques also leave a lot to be desired.

7. The "eavesdropping" came to light when one oil company found itself continuously loosing out by a small amount on bids for oil leases in Alaska. Investigating why the differences by which it underbid continued to be small, it discovered that its communication link between Houston and Alaska, where the bids were tendered, was being tapped. The company and other now encrypt or scramble much of their sensitive data, i.e. test and exploratory well results.

8. For background information on packet switching see the Task Force's background Report or Computing Trends: A Review of Computer/Communications Technology.

9. Some of the types of vulnerabilities that exist include the following:

- erroneous or falsified data input;
- misuse by authorized end users;
- uncontrolled system access;
- ineffective security practices for the application;
- faulty system security;
- procedural errors within the EDP facility;
- program errors;
- operation systems flows; and,
- communications system reliability and failures.

Basically any occurence, accidental or deliberate which results in a compromise of data confidentiality, integrity or access indicates a vulnerability.

Specific risks include:

- failure to satisfy one or more users;
- failure to satisfy external requirements (i.e. legal, regulatory, inter-organization, intra-organization, internal and external auditor needs, etc.);
- inadequate controlled systems;
- exposure to fraud and direct financial use;
- loss of accountability and the ability to reconcile data;
- unecessary or excessive costs resulting from over design of system or system reports;
- loss or misuse of resources;
- delayed implementation schedules; - admission of errors into the system in the form of erroneous or duplicated work, or outdated records;
- elimination of vital recordds from the files;

- introduction of unauthorized and possibly fraudulent transactions into the system;
- alteration, destruction, or disclosure of data in an unauthorized manner; and,
- direct or indirect financial loss arising from difficulties in reconstructing financial or other information assets as well as disruption of operations.

Insofar, as the computer system application allows for remote access over other than dedicated and trusted communication ports, these vulnerabilities and specific risks have a TBDF dimension.

10. Report on Computer-Based National Information Systems: Technology and Public Policy Issues, U.S. Office of Technology Assessment, Washington, D.C., 1981.

11. See below Chapter D.4 Computer Crime.

12. "Using Personal Computer" Research Report, Videotex Planning Service, Link Resources Corporation 4(Second Quarter, 1982)2 based on the IDC Survey of Desktop Computers).

13. The Growth of Computer/Communications in Canada, Computer/Communications Secretariat, Department of Communications, March 1978, with adjustment for 1985.

14. Evra Corp. f/k/a Hyman-Michaels Co. V. Swiss Bank Corp. United States District Court of Illinois, No. 73-6-2643 filed May 12, 1981. The case involves an instruction by Hyman-Michaels Company to its Chicago Bank, Continental Illinois to make an installment payment on a ship charter. The deposit was to be made at Swiss bank. The federal court found Swiss Bank in breach of contract and negligent in its failure to execute the wire transfer. In retrospect, it seems that none of the safeguards that Swiss Bank could have implemented to avoid this liability were sophisticated or expensive. The court stated "the burden of guarding against such a possibility is minimal in view of the potential injury involved". (See further, "Corporate Electronic Fund Transfers: Increasing the Stakes" The Scott Report, October 1981 and the Report on Legal/Jurisdictional Issues of the Task Force.)

15. For example, those in London and Glasgow participating in a computer time-sharing system based in New York can via New York communicate with each other, i.e. "domestic electronic mail", a service normally the preserve of the PTT.

16. On 18 April, 1982 a bombing by Basque separatists of one of the main telephone exchanges in Madrid not only put some 720,000 domestic circuits out of action but interrupted international circuits as well.

17. See below Chapter E.1.b.

18. A computer programmer in California, Lewis DePayne, has been placed on three year probation and given a five month county jail sentence after pleading no contest to charges that he illicitly used a San Fransisco-based system belonging to U.S. Leasing International, Inc. DePayne had broken into Pacific Telephone Co.'s local computer centre stealing sensitive systems documents, including password lists and technical manuals. This he (or his collaborators) used to penetrate the telephone company's mainframe and illegally alter some of its key data. DePayne was described by a local district attorney, Clifford Garrot as a "latter day phone freak who delights in finding out access codes, electronically breaking into systems and sabotaging their data. Phone freaks consider electronic vandalism a personal challenge". Apparently, DePayne publicized the confidential material through various electronic bulletin boards. This know-how was then used by others to change the phone company's billing data, enter fake stop orders and otherwise wreak systems havoc. According to Garrott, it seemed that the ultimate goal of DePayne and like-minded cohorts was to shut down the entire phone system in Southern California. (Computerworld, 28 June 1982, page 7).

19. See Appendix C for background information on encryption and related issues.

20. Tom Wylie and Donn B. Parker, "Computer Crime", Proceedings of the International Computer Crime Conference, sponsored by the Continuing Legal Education Society of British Columbia, October 1981

21. Jay Bloombecker, "International Computer Crime: Where Terrorism and Transborder Data Flow Meet" Computers and Security 1(January 1982)1: 41-53.

22. Command Paper on the recommendations of the Security Commission, presented to the House of Commons by the Prime Minister, United Kingdom, 21 May 1982. This is the public summary of the Full Report (which remains secret) resulting from a review of security procedures and practices currently followed by the public service by the British Security Commission (Chaired by Lord Diplock).

23. In contingency planning, the possibility of temporary off-site storage and processing is the most common approach. This involves finding a data centre with a computer configuration similar in nature to ones own and one which is ameniable to guaranteeing to provide a certain amount of processing at some future. Finding a compatible data centre is difficult, but finding one which will guarantee sufficient surplus capacity to handle its own plus an additional work load is impossible. Firms have now appeared, in greater numbers in the past two years, which specialized in the provision of back-up facilities.

    They offer services ranging from off-site locations (available to a limited number of organizations) to fully operational data centres that can guarantee that within hours the client is back in full production. The growth of new etrants into this industry indicates that it is a response to growing recognition of vulnerabilities of data centres.

Apart from having back-up in the area of processing, and data storage, arrangements may need to be made for back-up communication nodes in the network. If one uses vendor-supplied value-added networks, one usually has device and protocol independence. Even if one uses a private leased network, back-up involving a public switched network may be required as well as the ability to establish a dialed connection whenever the leased link fails. In any event, maintenance of the previous security profile may be difficult if not impossible.

One back-up facility firm indicated that a number of factors favour having the back-up facilities for companies close at hand. First of all, it is already difficult to regenerate a facility at a remote location. The further the back-up facility is away from the host data centre the greater the logistical problem of moving data, people and supplies. For the users with remote or link-up terminals the closer one is to the host data centre the easier it is to establish back-up communication facilities. Should the back-up facility be another country there might be a need to move hundreds or even thousands of tapes across the border(unless duplicate data is regularly maintained at the back-up site). The paperwork involved with custom clearances alone would present a formidable challenge. In addition, one would be moving outside of the local or national data communication network, which would require the users to become acquainted with new communication protocols and procedures.

24. Finally, any corporation with many data centres can provide back-up by ensuring that redundant processing capability always exists to handle the loss of any one facility. If the corporation is an MNE, it is logical to include all computers in the back-up net. This means that data must be moved continuously to maintain the contingency plan. For more detailed review of data retention and storage requirements consult the Task Force Report on Data Storage and Data Retention.

25. The criteria for selection of the location of the back up site should be that it is not subject to the same exposure to specific threats as is the principle site, e.g. not in the same earthquake fault.

26. Electromagnetic pulse or EMP was first encountered during the early days of nuclear testing when some cars parked in the vicinity of the test site failed to start despite the lack of any serious visible damage. It was later discovered that EMP occurs if the atmospheric conditions and the shape of the nuclear bomb create a detonation whose expansion is not perfectly spherical then the differential ratios of the rapidly expanding blast sets up a potential difference, i.e. a very brief pulse of very high voltage that can be picked up by anything that will conduct electricity. In addition, the gamma rays produced by a high-altitude nuclear blast would hit atoms in the atmosphere generating a wave of high-energy electrons.

A scenario predicts that a single nuclear bomb designed specifically to maximize the EMP effect, detonated at a very high altitude, i.e. 100 miles, could do untold damage that has very little to do with explosions, fire storms or radioactive fallout.

A nuclear weapon detonated at an appropriate altitude would produce an EMP generating tens of thousands of volts at the points on the earth's surface where it hit. Considering that lightning generates only tens of thousands of volts and that sensitive microchips can be burnt out by less than one millionth of a joule, EMP would cripple electrical power stations by blowing circuit breakers, the energy burst overwhelming surge arresters designed for lightning. EMP would also put many power starting out because they too are computer controlled. Most vulnerable to EMP are all microelectronic-based products and services.

The principles involved in protecting against EMP are not complicated, i.e. it is a matter of adopting the principles of Faraday's cage.However, in practice this can be extremely difficult. EMP countermeasures include trying to "harden" communications gear against EMP with super surge arresters, shielding and redundant systems (The Boeing 747 Doomsday Plane At Andrews Air Force base to be used by President Reagan in case of emergency is said to be EMP "hardened"). But most systems will not be shielded against EMP simply because few people will spend that much money to guard against something that has never happened, might never happen and might not generate the worst case scenario even if it does happen.

The U.S., however, is taking EMP very seriously. In his message to Congress, (early February, 1982) President Reagan noted that in terms of defense, he had found "serious deficiencies" in current communication and warning systems which are "vulnerable to severe disruptions from an attack on a very modest scale... especially in the event of use of nuclear weapons". Consequently out of the $215.9 billion allocated in the U.S. budget for FY 1983 for the Department of Defence, $23.2 billion is authorized for strategic programs including long-term continuation of improvements in the survivability of warning and communication systems.

27. Fibre optics is a method whereby light pulses are used to send a digital signal by bouncing them off the interior wall of a slender glass fibre. Not only do fibre optics offer a high quality transmission, they are also more secure, both the line itself and at the relays, e.g. from EMP. For the signal to be interrupted the line must be tapped which can not be done in the ordinary sense, i.e., picking up the electromagnetic radiations. Instead the line must be cut temporarily to install a "mirror". No matter how fast the cut is made and the tap installed, a continuous check signal for line integrity would alert the users to such an attack. There are no TBDF implications here as yet for TBDF since no fibre optic cable crosses the border or is being planned. It bears monitoring, however, since along with cable, it may provide secure alternatives to the rather high speed data transmissions involving satellites. They can also operate at extreme bandwidths.

The Northeast Light Corridor Project Refers to a 776-mile fibre optic telephone network linking Washington, Boston and New York. For the first 404-mile portion, AT&T asked for bids and Fujitsu Ltd., a major Japanese corporation, came in as low bidder while meeting all the technical specifications. However, AT&T was forced to reject Fujitsu's bid for "national security" reasons, the argument being that "these networks in

the fibre-optics link-up are the main arteries of communication" and acceptance of the bid would "establish a foreign corporation as the essential operator of our (U.S.) sensitive communication network". Later on, it was found out that on closer inspection the "national security/ sovereignty" argument did not hold up but Fujitsu nevertheless was not awarded the contract.

28. An information resource can be considered a source of data or set of data, the existance (or ownership?) of which can be considered an asset having economic, cultural, social and/or intellectual (property) characteristics. It suffices to say that generally data can be considered to be collections or groupings of observations and/or facts while information consists of data (and other information) in analyzed or ready to be analyzed or useable form. Information reflects the synergistic combination of medium and message. Further, depending on its use data can become information and information can become data.

29. For details, see Electronic Data Processing Security Standards and Practices for Departments and Agencies of the Government of Canada, Government EDP Standards Publication GES/NGI-14, June 1980 (under revision).

30. For details, consult Chapter 440, Section 8 "EDP Security" in the Administrative Policy Manual, Treasury Board Canada, as well as Security in the EDP Environment, Security Information Publications, RCMP, 2nd edition, October 1981.

31. For a further discussion see the Task Force project Report on Legal Aspects of Transborder Data Flows.

32. Idem.

33. The Swedish government study found that the lack of awareness of security and vulnerability was widespread, and that the significance of education in relation to vulnerability questions cannot be ignored. It concluded that the vulnerability of existing computer-communication systems and networks could be limited, but that information, consulting and raising of awareness of vulnerability problems was not enough." A draft was prepared of a proposed Vulnerability Act which would inter alia,

- put responsibility for vulnerability questions on the user of service bureaux;
- make the examination of vulnerability factors an integral part of vulnerabilities addressing not only the use of hardware, software and communications but also permissable contents of data banks and to what extent processing may take place abroad.

As a result of the work done by SARK and the acceptance of its findings that "vulnerability is unacceptably high", the Swedish government appointed (July 1981) a Vulnerability Board (SARB) to serve as an advisory and consultative body on matters pertaining to security and vulnerability in the context of computerization and data. Concerned with both the

private and public sectors, the Board includes representatives of national and local governments and the business community. SARB developed an action plan which was accepted. The main components of the plan of interest to our discussion include:

- development of methods for testing vulnerabilities
- the undertaking of a continued and more profound analysis regarding - EDP dependence on foreign countries
  - vital data processing taking place outside Sweden
  - effects of external disturbances, etc.
- assessment of the increasing tendency to concentrate skilled manpower for technical maintenance at foreign service centres
- investigation of people-related factors such as risk of criminal acts, terrorism, act of sabotage.

APPENDIX "A"

SHORT REVIEW OF COMPUTER SYSTEMS VULNERABILITY FACTORS

This Appendix contains a short review of computer system vulnerability factors in terms of

- the operating system;
- the data in a system; and,
- the disruption of an operation or application i.e. contingency planning.

1. Operating Systems Security

It has been shown that no general technique can be developed to prove that a system is secure. Whereas a piece of machinery can be tested and approved, software by its variable nature must undergo constant review. Even computer hardware is produced as many copies of the same model. For software this is true only for the so-called "canned" software. However, specific systems can be designed to provide certain levels of security and /or protection against known attacks. The significant computer security problem lies in the software that is supposed to fill a role in enforcing security by utilizing the hardware attributes. The major emphasis is usually on operating systems but it must be recognized that other forms of software can and do play a critical role in security, i.e. special software subsystems such as data management, transaction systems or even micro-code that provide security over and above that provided by the operating system. A number of approaches are worth noting.

a. Kernelized Secure Systems

Many attempts to formalize the approach to security of a computer system centre around defining subjects, i.e. users and programs, and objects, i.e. systems programs and data, and the permitted access or linkages between each subject and object. These security measures thus involve establishing the rules defining subject-to-subject access. One mechanism for ensuring this is a reference monitor. In order to provide security in a system, one can implement a reference monitor concept which requires that there be security mediation for every access between a subject and an object. The implication of this requirement on conventional computing architectures has been to establish a centralized body of code, often referred to as a "security kernel" which alone performs this unique mediating function. A security kernel is the software portion of the mediator or reference control monitor and access control mechanisms. A security kernel is a small, isolated part of the system at the lowest level of functionality which contains all the security enforcement code. In association with the hardware, the security kernel acts as a reference monitor which takes all the security relevant decisions. Current research efforts in kernelized secure operating systems have

developed some experience in the software tools and management approaches that seem necessary, e.g. KVM/370/Kernelized VM/370), KSOS (Kernelized Secure Operating System), UCLA Secure Unix, PSOS (Provable Secure Operation System) as well as Honeywell's MULTICS GUARDIAN effort. A major research project on the use of kernels in the U.S. suffered from lack of funding but an even more ambitious project supporting various data models and intended as a secure meta-DBMS is currently underway in Germany. The development and demonstration of trusted computer operating systems including KSOS and KVM/370 is recent with test installation starting only in 1981. There are, however, two major drawbacks to this approach, namely, proveability and performance degradation.

b. Back-End Data Management System

This approach involves an architecture consisting of a small network of dedicated single-level computers with a central computer having a secure operating system. Each small computer runs its own data base management system accessing only its own data bases and can be accessed itself only via the computer with the secure operating system, which thus serves as a transaction processor. However, the small computer must, in general accept the word of the host as to the identity and authority of the access request and thus relies on the host security as well as its own.

c. Restriction of Priviledge Approach

This is an approach for a system which allows only for the use of a data management system with general programming not being permitted. The vulnerability in such a system lies in the need to ensure that the application programs contain no time bombs or trap doors.

2. Data security

While operating systems emphasize protecting the computer at the system and data base levels, other methods are available to protect the data within the data base itself. The methods used vary in accordance with the priority and need to maintain data integrity, i.e. ensure that the data does not differ from the original source and has not been accidentally or maliciously altered, disclosed or destroyed.

The vulnerability of the data varies with its inherent sensitivity. Sensitive data require a degree of protection due to the degree or magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration or distruction of data (e.g. proprietary data, personal data, well exploration data, as well as national security, intelligence and law enforcement data). A "sensitive application" is, therefore, a computer application which requires a degree of protection because it processes sensitive data or because of the risk or magnitude of loss or harm that could result from improper operation or deliberate

manipulation of the application such as in automated decision-making systems.

The vulnerability of data varies with its inherent sensitivity. This inherent sensitivity is a function of a number of variables, e.g. quantity, context, age, and degree of analysis, and, of course, data content.

a. Quantity

The sensitivity of data increases with quantity along an "S" shaped curve, i.e. the sensitivity increases more slowly with quantity for large quantities. This is because large quantities of data start to look like noise. The vulnerability of data on a particular medium will also increase with its density.

b. Context

The sensitivity of data varies with its context. It tends to increase along with the number of distinct associations such that "A" and "B" taken together are significantly more sensitive than either one alone and adding "C" can greatly increase the sensitivity of both.

c. Age

In general, the sensitivity of data decreases with age (there are exceptions).

d. Degree of Analysis

In most cases, the sensitivity of data increases with the degree of analysis or interpretation such that raw data is less sensitive than organized data which is less sensitive than the conclusions which may be drawn which in turn are less sensitive than plans of action, i.e. degree of associability (inference).

Within a computer system a number of possible approaches exist to reducing the vulnerabilities of the data itself. Several of them are given here:

a. At Data Base Level

Here each data base is assigned a classification equal to that of the most sensitive data it contains and access to the data base is permitted only to these who are permitted to access the sensitive data. However, such an approach can easily lead to over-classification of most of the data in a data base.

b. At the Record Level

Under this approach each record within a data base is classified according to the highest classification level of the data it contains resulting in a true multi-level data base application. The classification of each record is determined at the time of its creation. It should be noted that the rules for raising classifications of records (i.e. causing them to disappear from the view of users not having sufficient clearance) and for lowering classifications of records (causing them to appear into the view of some users) may have complications on account of security policy constraints or because of the possibility of users making inferences as a function of whether they can see a particular record or not. It also relies on the integrity of the operating system and subsystems.

c. At the Field Level

Records are composed of a number of discrete fields. For relational data base management operations, classification at the field level has a certain appeal. Each collection of fields of the same classification can be stored in a file of that classification along with the key to the records. One can create fields with different domains at distinct security levels and without encountering the problem of records appearing or disappearing as noted in the previous section. Here also, the integrity of the operating system and subsystems is a key factor.

d. Priviledged Program Control

This is a means whereby users who are not permitted to have direct access to information in a data base can, by using a priviledged sanitization program, perform certain functions, i.e. one can only do statistical abstracting or compilation. In this case the operating system and subsystems integrity must be maintained at the user level. Certain forms of penetration are still possible here especially by those users who being conversant with the principles of statistical interference may be capable of infering certain information contained in the data base itself. Consequently, there may be a need for a control program that limits or interprets the maximum number of "statistical" queries by a user at a single session and then derives access to the system for a certain period of time.

e. General Access Control

This is the most general of all forms of data classification. Generally, this involves establishing a set of access-control tables associated with the profile of each user. i.e. what data bases, records, fields with records, etc. a given individual can have access to. The weakness in most of these systems is that often the access tables are treated as normal data and thus can themselves be accessed and altered.

f. Data Sharing Controls

This involves protection against anomalies resulting from concurrent usage of the same data, e.g. deadlock, lost updates. Data security problem can occur when specific data are being accessed and updated simultaneously by different users.

g. Encryption

While one normally encrypts data as they are being transmitted, sensitive data can also be rendered less vulnerable to attack if they are stored in the data base in encrypted form. However, this approach may introduce data retrieval and processing difficulties. Even then, the data usually must appear in the clear during processing and for input/output operations. (For more information on encryption methods see appendix C).

3. Contingency Planning and Vital Records

Contingency planning includes emergency planning, back-up plans and recovery plans and, of course, the identification of vital data.

Organizations of any size of importance usually have plans in place for identifying and containing the damage that might be associated with catastrophic or man-made events.

a. Back-Up Plans

In the event, that damage occurs of a nature so severe as to deny the use of the system for an extended period of time, there is a requirement for alternative means to satisfy the requirements normally met by the system. Apart from the subsitution of manual procedures, back-up plans usually involve arrangements whereby a computer operation is transferred to a similar system either within the organization or elsewhere.

Organizations need to define the scope of their contingency plans which must be predicated on the total destruction of the data processing centre. The back-up option which is the most effective, but also the most costly is that of using two data centres. Centres with multiple CPU's at the same location, or if elsewhere within the communications network, can be used for partial or total disruption.

The possibility of temporary off-site location is the most common approach. For a long time, this involved searching for a data centre elsewhere which had a similar configuration and operating system as that of the data centre. Such mutual assistance agreements are the least costly but also the least effective unless test are run to ensure the portability of large application from the one system to the other. The fact that in the 1970's like data centres were difficult to find nearly led a number of Canadian firms to rely on

data centres in the U.S. for back-up. However the probability of finding a similar configuration in Canada is greater now than in the past.

For back-up purposes, each user may make arrangements for different resources for back-up and each user could have multiple choices. User A may have available several other (similar) installations in the same community, user B may make arrangements with two or more data centres, user C may have a manual back-up, user D may have a contractual arrangement with a data centre specializing in back-up assistance, while user E may plan for any combination of these.

Apart from having back-up in the area of processing, data storage, arrangements may need to be made for back-up communication nodes in the network. If one uses vendor-supplied value-added networks, one usually has device and protocol independence. Even if one uses a private leased network, back-up involving a public switched network may be required as well as the ability to establish a dialed connection whenever the leased link fails. In any event, maintenance of the previous security profile may be difficult if not impossible.

The past two years have seen the appearance of a greater number of companies specializing in the provision of back-up facilities offering services ranging from off-site locations (available to a limited number of organizations) to fully operational data centres that can guarantee that within hours the client is back in full production. Members of this industry indicated that their entry into this field of operations is in response to growing recognition of vulnerabilities of data centres, the importance of the data centres to the organization and the resulting need to minimize disruptions in operations.

A number of factors favour having the back-up facilities for companies close at hand. First of all, it is already difficult to regenerate a facility at a remote location. The further the back-up facility is away from the host data centre the greater the logistical problem of moving data, people and supplies. For the users with remote or link-up terminals the closer one is to the host data centre the easier it is to establish back-up communication facilities. Should the back-up facility be in another country there might be a need to move hundreds or even thousands of tapes across the border. The paperwork involved with custom clearances alone would present a formidable challenge. In addition, one would be moving outside of the local communication network, e.g., Datapac, which would require the users to become acquainted with new communication protocols and procedures.

Further, except in the case of coaxial cable or fibre optics, transmission rates of terrestial networks are too slow to allow the transfer of whole data bases in the face of an impending emergency

unless a set of back-up data in the form of magnetic tapes of diskpacks is already maintained at the back-up facility as part of contingency plans.

c. Vital or Essential Data

Apart from taking measures to ensure continuance of operations, most organizations have in place a program for the preservation of essential data to ensure continuity of the organization in times of an emergency. The availability at the right places and times of those data, absolutely essential to the carrying on of the business of the organization, determines to a considerable degree the extent to which the organization can continue to function. One of the most difficult aspects of a vital records program is that of selecting essential, not merely desirable, data to provide the information required by an organization during or subsequent to an emergency.

Determining what is to be considered, vital data include the analysis of the appropriate laws, regulations and financial/audit requirements as to which information the organization is legally obliged to maintain. It also includes determining which data essential to the reconstruction phase to re-establish the organizational pattern and the basic functions of the organization, i.e., essential information such as that pertaining to operations, administration, organization as well as technical and research data.

Today, data can be made easier to recover because computers produce clear copies of data, which are inexpensive to reproduce and which are portable. Unlike records in hard-copy form, machine-readable data is of no use unless it can be interpreted and processed. For machine-readable data to be utilizeable at another centre therefore requires accompanying documentation, the necessary software programs and job control language.

Usually, the system operations group, and in some cases the data administration area if it exists, is responsible for back-up and recovery of software for programs and data and for the integrity of programs and data as supplied to it.

APPENDIX "B"

SUMMARY OF METHODS OF UNAUTHORIZED ACCESS TO AND USE OF COMPUTERS SYSTEMS AND METHODS FOR REDUCING SUCH VULNERABILITIES

This Appendix contains a short review of vulnerabilities introduced into computer systems having remote access facilities, methods used to gain unauthorized access and methods for reducing such vulnerabilities. In particular, the appendix reviews:

- the dial-in or log-on procedure;
- techniques used to gain unauthorized access to data or software;
- techniques used to execute unauthorized activities on a system; and,
- some vulnerability characteristics of the terminals themselves.

Access to computer systems via remote terminals using communication networks present difficult security problems because they involve undefined physical space and undefined persons (or personnel) who might be able to get access to a computer system. The security challenge thus becomes that of controlling access by an unknown person, located in an unknown place and having unknown levels of skills and resources. From a technical point of view as well as in practice, there is little distinction between attempts at unauthorized access from within a country or from outside the country of the host computer system, especially where the communication network allows direct long-distance dialing or interlinked digital transmission networks.

Before launching into a discussion of methods employed to gain unauthorized access to a computer system, a brief discussion of access control is in order. While access controls include the restriction of physical access to particular equipment this discussion focuses on the question of electronic access to the operating system and the data contained therein. The three major areas of access control policies are:

- identification, i.e., the process that enables recognition of legitimate users or resources as identical to those previously registered with the computer system, generally via the use of machine-readable names or codes;

- authorization, i.e., the process of granting to a legitimate user, a program or process, the right of access at the appropriate level. Separate authorization could be provided to different categories of users with varying levels of access privileges, types of access (e.g., read, write, append or query only) or to specific programs and procedures. In some cases, file level access controls will not suffice in light of privacy considerations where record or field level controls are often necessary; and,

- authentication, i.e., this includes measures to increase protection against fraudulent access by establishing the validity of a transmission, a message, a station or the identity of an originator.

Threats can be divided into natural and man-made and the latter category into unintentional and intentional, i.e., mischief, theft, fraud, sabotage, embezzlement, vandalism, wars and other activities resulting in data conversion. A number of methods have been developed in gaining unauthorized access to a computer system via a remote terminal but first of all it is necessary to establish communications with a computer system.

The process of establishing communication with a computer system from a remote terminal is called "Log-On". The capability of establishing communication with a computer is normally carried out via a dial-up using a commercial telephone facility. From a TBDF point of view, one can for all intent and purposes establish a connection with any computer allowing a dialled connection, where and whenever one can establish a telephone connection. Private leased lines, terrestial or non-terrestial are not considered "dial-up" unless one can access these via a public network. Dial-up may consist of manual or automatic dial-in, automated answering/response, automatic switching or re-routing. Having dialed-up, the user must identify himself (and the terminal) by entering combination of codes, passwords and/or knowing procedures which allow the system to authenticate the user and allow him access at the appropriate level. This procedure is usually called "log-on".

Systems having this capability are susceptible to attack from remote locations and therefore may involve TBDF considerations. Since the price of a terminal or micro-computer with a modem is not high and can be acquired very easily, any person could use these facilities to "attack" a computer-communication system either methodically or on an ad-hoc basis. Identification and authentication codes or parameters that are required can be "discovered" or perhaps can be generated until the correct access combination is attained.

Generally speaking, dial-up poses a growing threat to dial-up EDP facilities. Consequently, EDP systems containing sensitive data often do not possess such capabilities or else contain elaborate security checks. In a number of instances, not allowing dial-up facilities to a computer system is an extension of an organization's policy of restricting access to all or parts of its information regardless of whether it is in hard-copy or electronic form. Vulnerability is thus reduced by not allowing or severely restricting remote access.

Precautionary methods against unauthorized dial-up and log-on usually include suppression of display/printing of any of the codes/passwords entered, minimizing the number of false tries, time delays between entry of unacceptable codes or the dropping of the line to prevent computer generated unauthorized access attempts. Automated terminal (as opposed to user) identification is another precautionary measure (especially where transactional services are involved). As stated

earlier, a system with a "user-friendly" approach with "help-tables" gives an insight into hardware, software and related system to a would-be penetrator. Identification and authentication codes and procedures are changed where appropriate and have limited distribution thereby minimizing "accidental" discovery. Other precautionary access mechanisms include magnetic cards, voice or finger/hand identification at times in combination with (encrypted) personal identifiers.

Consistent enforcement of access rules is necessary even if this includes the keeping of records specifically for this purpose. Such records often include a log of all attempted accesses to the system distinguishing between those allowed and disallowed to and with a monitoring program which would provide the appropriate alert those responsible for the security of the computer system.

Having gained unauthorized access to a computer system, a number of techniques are used to gain access to the data or software or to execute unauthorized activities on the computer system. These include:

a. Browsing and Scavenging

Browsing is the scanning of available processes and data in an attempt to identify and exploit sensitive data usually using normal access facilities.

Scavenging is a more deliberate form of browsing whereby residual information on system files in temporary storage or ready to be re-allocated and transferred back to secondary-storage is read (and recorded) by a person who normally would not have access to such data.

Quite often, end-of-data markers are not always inserted immediately or space is allocated without restriction and not erased immediately after reassignment. In addition to normal file access controls, corrective procedures include ensuring that files are properly marked and temporary space is erased immediately after use.

b. Eavesdropping

Eavesdropping could be considered a special case of browsing characterized by the fact that the attacker is outside the controlled environment. Examples might include observing a CRT from a distance using a telescope or collecting acoustic emanations from a telephone or typewriter by the use of a parabolic microphone or wire tapping.

Eavesdropping techniques do not provide direct access to a computer system but use passive means to obtain the information necessary to penetrate the system or by establishing a means for observing the

system, learn what data exist, and flow and the manner in which they are being processed. The object is to intercept, store and subsequently analyze data as they are being processed or communicated. Generally speaking, domestic laws do restrict use of wiretapping equipment or the interception of signals. Wiretapping can be prevented by encryption.

c. Exhaustive Attack

An exhaustive attack is a method whereby a would-be penetrator gains access by trying all the password or encryption key possibilities. For example, one can discover a correct password providing that one is able to try enough different possible passwords and the system allows multiple tries. An intelligent terminal or micro-processor can be programmed to carry out an exhaustive attack on its own.

d. Spoofing/Posing

Spoofing or posing is an attack in which a person or process pretends to be a more priviledged person or process. Specifically, spoofing refers to a user thinking that he is interacting with the host system while in reality the user is under the control of a program of the penetrator. The goal of such an attack is to have the authorized user provide such information (access codes, procedures and/or data sets) which will allow the penetrator to carry out an unauthorized access utilizing these same privileges.

e. Trojan Horse

One of the most important methods of attack used by determined penetrators to subvert a computer system is known as a Trojan Horse attack. A Trojan Horse consists of a program or routine which is usually imbedded in a larger program (operating or application systems) which if certain predetermined conditions are triggered or criteria are met, will perform specific tasks. A Trojan Horse could thus well be a computer program which performs a legitimate task but which has illegitimate side effects. A Trojan Horse is used for those attacks which are planned to take place at some time in the future and which can involve either an authorized or unauthorized user.

Normally a high degree of programming expertise is required since the Trojan Horse tactic requires the placing of specialized routines during systems development or testing which become activated when the system becomes operational. Some examples of Trojan Horses include the University of Alberta students printing obscenities on Syncrude paychecks when the University Computing Centre processed the payroll. More serious instances involve the removal of funds from financial systems, or "revenge" by a disgruntled programmer by causing the system to crash "inexplicably".

(1) Trap Doors

A trap door attack is a special case of a Trojan Horse attack. It provides a secret door into a computer system known only to the attacker. Trap doors are thus weak points in a system (hardware or software) which can be exploited to bypass security features. Utilization of trap doors usually require detailed knowledge of the system. This can be acquired through a detailed analysis of the documentation, trial and error or collusion with system programmers. However, in some instances all that might be required is knowing certain transaction codes. In addition, an individual with working knowledge of one or more systems (hardware and software combinations) can take advantage off this in trying to penetrate similar systems of other organizations.

In the development of large application and operating systems, programmers often insert entry and exit points and procedures which assist in debugging, i.e. correcting errors in the computer programs. These are breaks in the codes that allow for insertion of additional codes or for intermediate exit/output capabilities. As a matter of fact most computer systems are designed to allow for easy access to sections of the source code by system programmers in order to facilitate the ability to analyse errors, undertake debugging and the making of modifications when required. In addition, a system operator could insert a specific code that will compromise program safeguards through a trapdoor during the debugging phase utilizing these when the system becomes operational to carry out unauthorized activities.

(2) Time Bomb

A time bomb is another special case of a Trojan Horse attack in which a hostile action or process is triggered by an event, at a certain time, which need not be under the control of the attacker. For example, a programmer might insert a code or process which is triggered by the time of the day clock of the system. Instances have occurred where an employee before leaving a company expressed his disgruntlement with that organization by planting a time bomb which one or two years later changed the annual updating of all records to an erasure or seized control of all I/O devices thereby bringing transactions to a halt.

f. Electronic Piggy-Backing

Electronic piggy-backing is a method whereby an attacker attaches his terminal to the same communications line as an authorized terminal through the telephone switching system. The piggy-backer uses his terminal when the authorized terminal is not in use if the computer system cannot differentiate between the two terminals. Another piggy-back method is the interception of the data communications, returning error messages to the authorized user while sending the

attached instructions to the computer which assumes that these originate with the authorized user. The latter method is very complicated and cases are very rare. Usually the data can more easily be obtained or modified through impersonation or masquerading.

g. NAK Attack

Computer systems often include a design feature that allow a user to interrupt a process, perform an operation and then return to continue the process or begin another. Poor system design often leave the computer system and data in an unprotected state during this time, e.g. partially written files are left open and are more easily accessed or tampered with. The name "NAK" attack is derived from the fact that user intercepts are commonly generated by the use of the terminal's Negative Acknowledgement Key.

h. Use of Priviledged Utilities

In order to operate a system, programs(utilities) are used to establish access codes and passwords, allocate and track use of the computer and storage space, maintain the system library, control the security features and operate the audit trail, diagnose hardware and software errors, etc. Often these utilities, apart from controlling access to data and to certain hardware/software combinations, can allow a knowledgeable user with access to bypass all controls, to overide any other system control, interupt or monitor any stage of processing and review the data contents of the computer. While the extent or power of such utilities vary between different installations, unauthorized access to such utilities leave a system very vulnerable to all types of attacks. However, normally many such utilities are routinely used by many users.

i. Asynchronous Attack

Asynchronous attacks are those which attempt to exploit the time difference between a defensive action (or reaction) by the system and the attack itself in order to multiply the effect of the defensive action.

The methods of unauthorized access mentioned above describes vulnerabilities of a computer-communication systems to attacks of a technical nature. However, as is the case with other security matters, the personnel in an organization can easily compromise any security system. Those working on system or application programming are often the only persons in the organization who are totally familiar with an elaborate and complex production program. Application programmers design procedures handling everything from financial transactions (cheques, invoices) to very confidential data. Means for carrying out audit and security procedures for program verification and certification normally are not applied.

System programmers normally have access to all the system software resources and source code and can therefore modify any portion of the operating system to carry out unauthorized if not illegal activities. They pose an even greater threat in that they have the ability to by-pass or erase system audit and security controls or modify the data in such a way as to escape detection by these control mechanisms.

Collusion can take place within an organization between employees in the computing centre, employee a legitimate user or an employee and a person external to the organization who then mounts a remote attack. Countermeasures include screening at the hiring stage and periodic and random employee checks plus the usual technical measures.

Where terminals are used for unauthorized access attempts, there are a number of characteristics of terminals related to vulnerability which might be noted, namely;

a. Intelligence

The vulnerability of the host system to an exhaustive attack is influenced by the intelligence in the remote device. For example, an micro-computer can be programmed to launch an exhaustive attack.

b. Emanations

The susceptibility of the computer system to the disclosure of sensitive data to eavesdropping varies with the amplitude of signal bearing emanations as a function of the total emanations of the same type.

c. Attachment Flexibility

Vulnerability will vary with the number and types of external devices supported by the computer system. In general, vulnerability will increase with the number of different types of terminals that can be used to address a given computer system as well as flexibility in different means of establishing communications.

APPENDIX "C"

ENCRYPTION AND OTHER SCRAMBLING METHODS AS A MEANS FOR REDUCING VULNERABILITIES IN VARIOUS TYPES OF DATA FLOWS

This Appendix provides a short review of encryption in general, the DES standard, the public key approach, and the general characteristics and methods for protecting analog, digital and other modes of data transmissions.

1. Encryption

From ancient times onward, individuals and states were sensitive to the possibility of important information falling into the hands of unwelcome parties while it was being transmitted, i.e., by a courier. A number of techniques were developed ranging from physical means, such as special links, to intellectual means such a secret codes and ciphers. Cryptology has relied in this century largely on mathematical processes which makes it especially suited to the digital communication environment of computing. During World War II there was a significant increase in the development of new encryption methods and processes. Since then and especially in the last decade, the enormous progress in mathematics and digital technology have made it possible for the development of, for all practical purposes, foolproof and reliable encryption devices designed to protect information as it is transmitted through a variety of communication facilities. Public knowledge of encryption techniques was very limited until about 10 years ago.

As a matter of fact, the intelligence and defence community is somewhat ill at ease with the development in recent years of the study of cryptology as a valid area of research. Those working in information theory and certain areas of operational research and mathematics are working towards the discovery of unbreakable algorithms as a scientific challenge. Consequently, the development of new and unbreakable algorithms is no longer restricted to national agencies (i.e, defence, intelligence, communication authorities). Research into new encryption schemes by academic and corporate scientists outside of governments, poses some difficult vulnerability questions, e.g. "What is the balance to be struck between the right of unrestricted enquiry in encryption research and the potential losses to national security and intelligence?" The publication of research results might encourage foreign countries and corporations to create new and unbreakable codes thereby cutting off not only code-breaking activities by intelligence agencies but also law enforcement, i.e., in the context of a legal wire-tap or the interception and opening of the mails. On the other hand, if these new developments are kept from the private sector, might national security and well-being not be threatened as economic intelligence and data transmissions are becoming a more and more vital part of the workings of business? The private sector would want to reduce the vulnerability of data, electronic mail, electronic funds and commodity and other information transfer systems.

In terms of advances in encryption techniques, two major items are worthy of note, namely, the establishment by the U.S. National Bureau of

Standards of a Data Encryption Standard (DES) and new or recent research into techniques based on the "Public-Key" approach.

2. Data Encryption Standard (DES)

In the U.S. in 1965, the Brooks Act (P.L. 89-306, "Automatic Data Processing and Equipment Act) authorized the Department of Commerce to begin work on "uniform federal automatic data processing standards", a responsibility which the Department assigned to the National Bureau of Standards. In the course of time, the Bureau began to look at computer security and by the mid-seventies asked for submissions via the Federal Register of data encryption algorithms for consideration as part of the U.S. Federal Information Processing Standards. The NBS was looking for an economical method of encryption compatable with a variety of computer-communication systems. Of all the responses, the only practical one seemed to be IBM's Lucifer scheme. Before adopting the IBM proposal, the NBS ran it past the National Security Agency, which interalia is responsible for code-making and code-breaking operations in the U.S. The result was that the NSA convinced IBM to reduce the originally proposed key size from 128 to 56 bits. This gave rise to the charge that the NSA did not want a publicly available encryption code that it could not break thereby limiting the agency's capability for eavesdropping on commercial transmission. Most experts agree that the 56-bit key size is more than adequate and if pressed one could encrypt twice for a total length of 112 bits. Current military key sizes are routinely 20 times larger than the DES. The algorithm became a U.S. Federal Standard on 15 July 1977 and is commonly referred to as DES. The DES is now adopted for use by the U.S. Federal Government agencies outside of the military and intelligence fields. IBM defended the reduction to 56 bits on the basis of economy as larger key sizes would require too much computer time and because the 56-bit key could be easily placed on a chip (using current 1977 chip technology). IBM's cooperation with the NSA in working towards DES with a reduced key led some tographic specialists to speculate that there might be some hidden "trap doors" in the code which if used would make it easier to break. The past years have seen considerable activity by specialists in testing the DES for statistical or mathematical weaknesses. The DES has proven to be quite robust, the debate has subsided, but not totally died, switching to other areas (see below) and the DES is now a recognized U.S. national standard and the most prevalent algorithm in use today.

To understand the debate over DES and other encryption methods for digital transmission, it might be useful to outline the basic workings of the encryption algorithm. The DES algorithm is used in combination with a secret 56-bit key to encipher data in 64-bit blocks. A 56-bit key yields a number of 2^{56} or 7.2×10^{16} possible keys. The algorithm works on data expressed in bits (coded impulses representing either a "1" or "0" or pulse or no-pulse). This stream of bits is then modified by the DES algorithm according to a specific key, i.e., a 56-bit pattern, yielding a specific and unique outcome (output that is transmitted). To convert the data into code the DES uses two principal techniques, transposition and

substitution. Transposition is the changing of the order of the data according to fixed permutation. For example, a 8-bit transposition according to a permutation of 6,2,7,5,1,4,8,3 would change an input stream of 11010011 to an output of 01101110. The DES uses several similar and different transpositions. The other technique is substitution or the systematic replacement of one symbol by another. A look-up table is required here. Parts of the message are divided into small bit blocks and then assigned new values according to the table. The DES uses eight different look-up tables or "S-boxes" to govern the substitutions.

The DES thus uses various transposition and substitution schemes on each 56-bits of input in a series of complex computations dependent on the key. At the receiving end, the process is inverted to decipher the message, the DES algorithm and key being analogous to a combination lock. Even if the design of the lock's mechanism is public knowledge (which the DES algorithm is), it cannot be opened unless one has the combination. Similarly, the encrypted data remains secure as long as the key is kept secret.

DES has become a de facto standard. It has withstood various assaults and is vulnerable only to a direct frontal attack which is very costly. Alternate routes to obtain unauthorized access to commercial data protected by DES are probably more cost-effective for the private sector. National governments may have other than commercial motives in attempting to decipher encrypted messages.

The DES has been implemented in a semi conductor chip and is available for less than $100. Major manufacturers such as IBM, Motorola, Intel, Fairchild, Burroughs, etc. do offer DES-bound encryption either in providing DES-certified chips or systems build around the DES standard. Conern has been voiced by individuals in several countries about the fact that official control is being maintained by the NSA on the exportation of DES-based products, their export being subject to the U.S. Export Arms Control Act. This control justified in the name of national security is interpreted by others as constituting a substantial protectionist stance for the products and services offered by U.S. firms. While regulations do permit the export of DES products to Canada, so far only U.S. manufacturers are selling DES based encryption hardware. Some argued that such controls introduce a vulnerability and interfere with indigenous attempts to develop models and conduct experiments designed to specify encryption in communication protocols. But the DES algorith is public knowledge and is and can be implemented (even on microcomputers) by anyone with a minimum of programming skills.

3. Public Key Encryption

The workings of encryption algorithms are controlled by a unique number or bit pattern usually referred to as an encryption key. The debate over DES and subsequent research led to the development of the "public key" system by the academic community. The "public key" or "two-key" system is based on particular one-way properties of prime numbers. The result was the

development of a situation whereby the ability to encode does not allow one to decode and vice-versa.

Such a method known as the RSA method has been developed by MIT scientists Under this two-key or public key system, the encoding keys for each of the parties in a computer-communication network can be recorded in a public directory. Communication with one of the listed parties would require looking up the appropriate key in the directory and encoding the message accordingly. The intended receiver would then use his private or secret decoding key to decode the message. In short, separate but related cryptographic keys are used for encoding and decoding. The sender knows and uses the receiver's public key for encoding the message while only the receiver can use the intended secret key, which is related to the public key, for decoding the publically encoded message.

The strength in any communication system lies in the protection of the encryption keys. However, each sender/receiver pair must be provided with equivalent keys so that they can send and receive encrypted messages. Key distribution is usually accomplished with a protected key distribution channel utilizing courier service, registered mail, or a secure (encrypted with another key) communications channel. In traditional systems, the key thus needs to be distributed in secret between two or more parties. Key control therefore is a vital element in reducing vulnerability of computer-communications.

However, this method only solves one part of the key distribution problem, i.e., the need for secrecy. While the public key directory need not be kept secret, it must be guarded against illicit alterations. Otherwise, an attacker could change the public keys linked to certain intended recipients for his own (for which he in turn has his own private encoding key) and thus only he would be able to decode the intercepted messages.

While there has been much talk about encryption, its use is not yet widespread. The total market for encryption devices (in the U.S.) is small, only some $70 million and it is not expected to increase to more than $180 million by 1991. The promulgation of DES did not trigger a big movement towards the use of encryption equipment by commercial and industrial users. However, past experience does indicate that often just one well-publicized case of substantial damange resulting from unauthorized access may cause a whole industry or sector to employ encryption techniques, e.g., the oil industry.

A recent study by International Resource Data indicates that most of the data, text and voice encryption activity is attributable to the military, the oil companies and certain other well-defined categories that were using encryption techniques already ten years ago. In the financial community the use of encryption has increased, especially for automatic teller machines where the data transmissions are encrypted so that telephone taps do not yield the vital combination of customer account number and authorization code. Encryption is not the solution to network and data flow vulnerability problems but it is one very important element.

4. Encryption of Analog Transmissions

Typical scrambling methods for analog transmissions include frequency inversion, band splitting and time-division multiplexing. Since most of these techniques rely on a single fixed code, it is possible for a determined, sophisticated attacker to quickly determine the code used and thereby understand the encrypted messages. All of these techniques are considered to be fixed code scrambling. It is also possible to employ dynamic code scrambling whereby the code permutations change continuously during transmission. However, the equipment used for dynamic scrambling is more costly than that required for static scrambling and the trade-off is therefore in equipment costs versus risk costs.

Of interest here in the TBDF context is the static scrambling approach taken in the U.S. towards subscription TV services. Most of the signals for pay-TV are transmitted via satellite in scrambled form and then picked-up and descrambled by the local cable TV operator (CATV). The CATV operator rescrambles the satellite signals for injection into the CATV network to be sent to the home along with other signals. The cable companies rent a descrambler ("black box") to subscribers willing to pay for this value-added service. However, some of the less sophisticated codes have been broken and the spread of illegal "black boxes" is worrying the industry. The advent of Direct Broadcasting Satellites (DBS) will generate a greater problem since the potential market for "black boxes" to descramble and thus pirate signals will be much greater. In both cases, the sender of the signal has two choices. Either he can change the code frequently enough to discourage the pirate "black boxes" or he can use more sophisticated scrambling and decoding techniques. Some companies, including those in Canada, are working on an intelligent micro-processor that will do both. The solution may lie in the "addressable descrambler which will not operate unless it has been turned "on" by another incoming signal or code with such codes (which could vary) being send to each authorized address several times a minute. The transborder data flow problem with DBS is that the footprint of such a U.S. satellite, like that of other U.S. satellites, covers a substantial portion of the Canadian population. The question, therefore, to be asked in the TBDF context is "What will be the economic impact of DBS on Canada and what will be the effect on cultural sovereignty?" DBS antenas will be cheap and small while one will probably be able to order the descrambler via the mail from the U.S. (using one's favourite credit card). Further, it should be noted that a significant number of present and future satellite relayed broadcasting signals will not be scrambled.

In this, Canada faces a situation much like those of the nations of Western Europe which already fall under the footprints of Horizon I, the broadcast emmission of the Russian telecommunications satellite, and the British originated commercial broadcast by Satellite Television Ltd. via a channel of the European OTS experimental communications satellite.

5. Digital Transmission

The basic telephone circuit is designed to transmit human voice frequencies which usually range between 300 and 3,400 Hertz (Hz). The normal required band width is 3,000 Hz. The common carriers provide three broad categories of capabilities: narrowband (sub-voice), voice grade and wideband. A typical voice-grade telephone line can handle data at the rate of 9,600 bits per second (bps). Since normally telephone lines are subject to a variety of noise and distortions, the effective usable rate for an unconditioned line is 1,200 bps. At a considerable increase in cost a special voice-grade channel can be leased from carriers which is specially conditioned to provide for higher transmission speeds of up to 9,600 bps. The latter require special lines other than the normal dial-up network, e.g., Datapac.

The basic difference in transmitting a voice message and a data message over common carrier networks is that data communications require a modem inserted between the data terminal and the communication network, the modem converting digital data to analogue and vice-versa at the other end. For a long distance telephone call (i.e., one which crosses the Canadian border), the number called is received at the sender's local central telephone office and then switched via the public switched network to the nearest central office of the part called, in order to establish a circuit between the calling and the called stations.

Eavesdropping can be accomplished either through wiretapping or the interception of signals anywhere along the transmission path. Dedicated private line messages are always transmitted over an identical route while it also occupies the identical segment of the radio spectrum. Therefore, once the eavesdropper "locates" the frequency of the dedicated circuit, he can install electronic equipment to intercept and monitor every message sent over the circuit.

Switched private lines present a somewhat greater challenge. If the eavesdropper is interested in all messages to and from a user of a switched private line service then his job is essentially the same as above except that all lines must be monitored. If only some messages are of interest the eavesdropper must use some type of screening or selection process or collect the incoming data from the actual receiver handset. With switched private lines and the dial-up network, the eavesdropper can select calls of interest since each call is preceded by a signal identifying the telephone number being called. By using a computer, the eavesdropper can easily monitor and selectively screen large volumes of messages. The computer can be programmed to search very rapidly for key words, names, subject titles and/or telephone numbers of interest. The same holds true for packet-switching as a computer can screen the address of each packet. The customer can encrypt his data but only the common carriers can encrypt the "address" of the transmission. Otherwise, transmissions would go astray, since the relay nodes would not be able to recognize the "true address".

6. Other Modes of Transmission

The past decades have seen the introduction of two means for electronic data flows not yet mentioned. Both use light pulses to transmit messages, i.e. laser and fibre optics. Laser transmissions are difficult to intercept since one has to be in the line of sight which, because of the nature of lasers, tends to be very small but they are sensitive to atmospheric conditions. Further, point-to-point transmission usually involves short distances with the sending and receiving devices on the roofs of buildings. However, lasers do offer high speed digital data transmission and in the TBDF context, it might be worthwhile to note that lasers can be used to link a domestic (low cost) leased-line to domestic leased-line in another country, i.e. short distance border-hopping, with a substantial saving over the party in question leasing an "international" high speed private line.

Fibre optics is a method whereby light pulses are used to send a digital signal by bouncing them off the interior wall of a slender glass fibre. Not only do fibre optics offer a high quality transmission, they are also very secure, both the line itself and at the relays, e.g. from EMP. For the signal to be interrupted the line must be tapped which can not be done in the ordinary sense, i.e., picking up the electromagnetic radiations. Instead the line must be cut temporarily to install a "mirror". No matter how fast the cut is made and the tap installed, a continuous check signal for line integrity would alert the users to such an attack. There are no implications here as yet for TBDF since no fibre optic cable crosses the border. It bears monitoring, however, since along with cable, it may provide a secure alternative to the rather insecure high speed data transmissions involving satellites. They can also operate at extreme wide bandwiths.

BIBLIOGRAPHY

[In preparation].