日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

“The Risks in an IT Economy”

by

Mitsuru Iwamura
Professor
Graduate School of Asia-Pacific Studies
Waseda University
Japan

The Risks in an IT Economy

Mitsuru Iwamura

Paper prepared for the conference on:

The IT Revolution and Security Challenges

Institute for International Policy Studies

Tokyo

11 December 2002

The Risks in an IT Economy

Waseda University

Mitsuru Iwamura

Introduction

The risks attendant to computerization are becoming a focus of concern. Of course, computerization does not create only risk. Computerization brings new wealth to society and can help avoid loss. However, as the relative importance of information technology in our lives grows, it is natural that we should look at the downside as well as the upside. The shift of attention from the positive aspects to the negative aspects of technology as it develops and matures is a common phenomenon.

Most people will agree that one of the major contributing factors to economic development in the Twentieth Century was the internal combustion engine. Yet, today the main focus of concern is not improving mechanical performance but controlling the effects of exhaust on the environment. This does not detract from the contributions of the internal combustion engine to the Twentieth Century. This is simply the result of a shift in the focus of concern as the contributions of the internal combustion engine become commonplace.

Thus, when we discuss what information technology holds in store for us, it is a natural tendency to start to face the risks instead of the benefits. It may be said that a technology has taken root and matured in a society only when the negatives aspects are discussed as much as the positive aspects.

Attack from Outside

When we talk about the risks of information technology, most people probably think of computer viruses. According to statistical data[1], most cases of unauthorized access to information systems involve an insider who assists in some way, but the threat of viruses and similar attacks has spread along with broader use of open network environments like the Internet. The traditional methods of defense, such as controlling access to the computer room, is appropriate for attacks from within, but viruses do not travel through the same physical channels that people do; they travel through communications lines to invade information systems. Needless to say, the formulation of policies to minimize loss caused by such attacks is a major issue in today's information society.

However, establishing security checkpoints internal to and external to an information system—a firewall—is sometimes effective, even against attacks through communications channels. Yet, the perfect firewall would require that the firewall administrator inspect every message that went in or out of the information system. This is not practical.

Yet there is a fundamental difference between firewall administration and controlling access to a building. That difference is the cost-benefit balance for intruders.

For example, let us look at an airport security check. The technology used there is not so advanced, and breaking through these defenses would not be terribly difficult. Yet, from the intruder's point of view, the cost of detection could be arrest, prosecution, and more, so the cost is quite high. Airport security is relatively simple, yet it functions well, generally because the penalty for detection is large.

In contrast, the most severe penalty for attempting to break through an information system firewall is, in most cases, a denial of access, with no financial or personal penalty to the attacker if he is detected. This makes it possible for the casual hacker to use a trial- and-error approach, which occasionally overcomes and renders powerless the firewall that cost so much money to install. This lack of balance between the cost of attack and the cost of defense puts the defender at a disadvantage in the battle over information system security.

This imbalance between the cost of attack and the cost of defense can also be seen in the propagation of computer viruses. A computer virus is a program in digital data format, and precisely because it is digital data it can duplicate itself on infected systems and become distributed over a wide area. Thus, the attacker can design an attack that affects a tremendously

[1] From 2002 CSI/FBI Computer Crime and Security Survey (Computer Security Issues & Trends, Vol. 8, No. 1, 2002)

large number of information systems for a tremendously low price. This could never happen in the real world. In the real world, it is necessary to keep in mind that when attacking others, whether with a gun or other weapon, the cost generally grows in proportion to the number of people attacked. However, since there is almost no cost involved in the duplication of digital data, it creates an imbalance between the cost of attack and the cost of defense. Even one ill-intentioned person with a virus created using a relatively simple technique forces a tremendous number of people to invest huge sums to defend against it.

In economics there is the concept of non-rival goods. Food, appliances, and similar products can only be used by one person at a time. However, use of knowledge, safety, or a beautiful view by one person does not prevent other people from also using it. Assets that possess this quality are called non-rival goods, and the computer virus, made up as it is of digital data whose duplication costs almost nothing, is one type of non-rival good, albeit with a negative utility. The fact that digital data is a non-rival good is a source of social protest on one hand—as evidenced by the problem of free file-exchange software—and a source of giant monopolies like the Microsoft Corporation.

As is well known, most of the computer viruses being spread over the Internet target the operating systems (OSs) and software applications manufactured by Microsoft. This may not necessarily be because the security design of Microsoft software is exceptionally weak. Since Microsoft has an overwhelming share of the personal computer OS and applications market, it is most efficient for virus creators to target Microsoft products. Microsoft's market dominance is most pronounced in computer programs, and since these are non-rival goods, it makes Microsoft products the easiest and most efficient target for computer viruses, which are also non-rival goods.

Microsoft's monopolistic position in the personal computer OS and major applications markets raises many questions from an anti-trust point of view. However, I believe that more attention should be paid to the general security of the information society. Undoubtedly, use of the same software that others are using on networked computer systems is a positive external factor which contributes to Microsoft's ability to hold a large market share, but it is also a mechanism that forces the cost of loss due to viruses onto the user. If software makers who have achieved a high market share due to externality were forced, through a systematic framework, to compensate their users, even a little, when their software was infected by a virus, companies would design products more carefully from now on, and it would drive them to think more about preventing virus infections[2]. Of course whether or not such a framework is

[2] The obligation to use exhaust purifiers in automobiles has driven the development of

necessary must be discussed with a view to minimizing the costs for all society, but with the amount of damage being caused by viruses today, such subjects should not be off-limits.

engine parts which give off less pollution. The damages provided for in product liability law are not intended to heal the wounds of the consumer, but to promote the creation of safe products. Demanding protection against viruses from software producers in the first place would have the same effect.

The Conflict with Privacy

The information system intrusion problem is not the only risk we should be concerned with in the information society. Consider customer information systems used by retailers for marketing purposes. These systems must be designed to prevent theft of a customer's personal data through external unauthorized access. From this perspective, measures to counter the risks in an information society must first guarantee that information systems cannot be used for anything other than their intended purpose. However, the major risk here is not information system invasion.

As the range of personal data collected widens, so too does its usefulness and its sensitivity. The information collected by one retailer for marketing purposes shows only one part of a person's life and is not extremely sensitive. Yet, if many retailer systems are merged to collect individual purchasing information from many systems, that information might be used to give an overall picture of an individual's life, which would be considered an intolerable invasion of privacy by many. The ability to collect and collate a wide range of information using info-communications networks gives new importance to information on commercial transaction data that, until recently, has not been considered important from a privacy perspective.

Information on each economic transaction carried out by an individual is just isolated information if the transactions are viewed singly. However, if this information is taken together, that individual's lifestyle, tastes, and tendencies, as well as other sensitive information, can be divined by extrapolation. This method of gaining personal data by putting together isolated bits of information is called profiling.

However, a wholesale ban on techniques like profiling will not necessarily resolve the problem. Profiling was developed for use in creating effective advertising strategies and managing risk. Precision marketing is efficient at offering us products that we desire, and we can borrow money from financial institutions in the form of consumer, homeowner, and other loans, because they analyze the data they have amassed and then extract common trends and characteristics from unique individuals, which enables them to predict how much money they can safely lend to which types of people. Medical charts are one of the most sensitive types of data, but since that data is collected and analyzed, unintuitive side effects of medicines can be discovered and the relationships between diseases and the environment can be revealed[3].

[3] Normally the side-effects of medicines, environmental influences, and similar elements do not present a high risk of disease when viewed at the level of the individual, which makes discovery in the laboratory difficult. The collection and analysis of a wide range of personal data is effective in discovering these types of

Looked at in this way, an argument can be made for the benefits of collecting and collating personal data.

Generally speaking, when there were many costs involved in building and operating an information system and the technology to connect to information systems across the network was not fully developed, indexing particular personal data on another system, while theoretically possible, was not practical. However, the progress being made in information technology is bringing this type of personal data collection within the realm of possibility. We have a tendency to focus primarily on the topic of protecting information systems from intrusion—that is, on security in the information society. However, from a broader perspective, we need to consider how to prevent the violation of rights, since the indexing and analysis of information are not necessarily illegal in themselves. From that point of view, the issue of privacy is more than the issue of unlawful intrusion into information systems, and should be considered in the context of a conflict of interest that is inherent in the use of information systems.

The problem is deciding which is more important, the threat to privacy or the societal benefits in the accumulation of personal data. The US and Europe have taken different directions on this issue, with the US leaning strongly toward a system that strictly regulates government use and handling of personal data while permitting the utmost freedom of use for economic purposes, while Europe strongly leans toward legislation requiring stricter protection of privacy in the public sector than in the government. The 1980 OECD Guideline (a guideline on privacy and the trans-border flow of personal data), which could be called the international consensus on the legal importance of privacy, defines privacy as the right to control information about yourself (the right to participate)[4], and is a clever method of controlling the conflict of interest in the use and protection of personal data.

problems.

[4] Specially, it says

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

to challenge data relating to him and, if the challenge is successful to have the data

By the way, Japan is in a state of confusion on the issue of privacy in the information society. The history of the right to privacy in Japan goes back to the 1964 “ Utage no Ato” incident in which a Tokyo District Court decision recognized privacy as a civil right. Later, however, news agencies fought this decision, warning that it could be used to regulate news gathering and restrict reporting of the news, and the right developed into a restriction on the use of personal data by the government. (For example, the “Law for Protection of Computer Processed Personal Data by Administration Organs” was enacted in 1988.) There is still no telling when the “Bill Regarding the Protection of Personal Data,” proposed in the Diet in March of 2001, will become law.

This bill loosely follows the aforementioned OECD guideline. However, the core of that guideline, the individual participation principle, is abstracted in a regulation which states, “when handling personal data, allowance must be made for allowing the person to contribute as they wish” (Article 8 of the bill). Instead, those handling personal data (that is, companies which handle personal data) are obligated to maintain the right of participation (Article 5 of the bill). However, news agencies are exempt from this obligation, and it required the creation of separate mechanisms for each of the government ministries and agencies which are supervising these companies to ensure that they are fulfilling their obligations. This structure is believed to have been adopted as a legislative gimmick in deference to the news agencies, who were opposed to this bill. However, it softened the stance of the bill and created a political blueprint for “the vocal minority and the indifferent majority.” In order to overcome this obstacle, we need to reopen the basic discussion and work out a solution to the problem of the collection, protection, and use of personal data in the information society.

erased, rectified, completed or amended.

Cross-Border Issues and the Regulation and Surveillance System Crisis

The cross-border problem brought about by electronic commerce is becoming a major issue. It is certain that electronic commerce—especially the development of electronic commerce over the Internet—has sufficient impact on us to raise our awareness of the difficulty of applying law to the cross-border problem. Distribution of content over communications networks has brought us face-to-face with a wide variety of problems, ranging from taxation to pornography. Internet-based securities trading has entered a world that was already sorely in need of a realistic adjustment of interests, as evidenced by the problem of out-of-area application of securities regulations, such as the Securities and Exchange Law.

The 1980s saw accelerated growth of communications networks using computers, but until the mid-1990s these network systems were almost universally constructed around a large central computer, using a structure that could be called a pyramid. Communications passing over these computer networks traveled from the originating terminal to the central computer, and then from the central computer to the receiving terminal.

In contrast, the Internet developed at a rapid pace in the mid-1990s, and it did not employ the pyramid structure architecture based around a central computer. All computers connected to the Internet send and receive messages as nodes of equal rank. However, for the people who monitor or regulate business processes over the network, this presented a new problem. Transactions involving exchange of data over a network without a central computer—like the Internet—could not be monitored or regulated easily; sometimes they could not be monitored or regulated at all. The problem of hollowing out supervising and regulating organizations will probably be easiest to understand if one considers the impact that the arrival of account settlement methods like e-money will have.

Electronic money is digital data which has been protected from copy or counterfeiting using the most advanced information-processing technology. When one refers to electronic money, people associate this with a plastic card, simply because the IC card is one manifestation of information-processing technology. Leaving that aside, when the IC card and PC become able to perform the same functions as the giant computers at the center of the on-line banking system, even distributed information-processing systems using small equipment will be able to achieve a standard of security rivaling that achieved using large computers. This development will increase the degree of encroachment by PC- and IC-based account settlement systems on the territory of account settlement businesses, which would not have existed were not it for large-scale computers and fortress-like computer centers.

This obviously creates a certain danger to the monitoring and regulating framework, which is based on the predominance of the central computer in information-processing systems. This danger extends to the various systems that were constructed on the premise of this regulating framework.

As long as the on-line financial systems of financial institutions (which comprise a typical pyramid network) are used for international fund transfers, data on the movement of funds between countries will be collected and recorded by a central computer. Thus, control of fund transfer between countries was easily effected by monitoring and regulating the center of operations at which this data was accumulated. For 50 years from the end of World War II, Japan's foreign exchange control policy—commonly known as the forex bank doctrine—fulfilled its inherited role of monitoring the movement of funds to authorized foreign exchange banks, and this too depended on the existence of the central computer data control architecture. Thus, if electronic money and its distributed Internet-like network is used for processing international fund transfers, it may lead directly to a crisis in the current law enforcement system.

However, the important point is, rejecting a product that is based on new information technology because it threatens the law enforcement system will lead to a bitter fight, arguments over the merit of the system notwithstanding. This is because the development of the info-communications network will do away with the concept of separate regional "markets" and will give birth to one huge global market. Under these conditions, regulatory authorities and law enforcement authorities will have to work together more closely than ever before.

Competition of Laws

Markets and information are two sides of the same coin. What we call a market is a trading place for people who share information. No market is possible where there is no information. Economists define wealth as possessions of economic value that can be traded, and markets as the platform where people who share information and have various interests gather and trade wealth. Thus, the narrower the range of potential information sharing, the narrower the potential market. In the era when the sharing of information between areas which were remote from each other was difficult, people collected in the cities and markets to share information. This created many markets within one country, and no one thought it unusual that the same commodity would have different asking prices in each market.

However, this situation began to change, slowly at first, but then rapidly, as info-communications technology developed. The first big change came with the beginning of postal services in the Nineteenth Century; the spread of the telegram and telephone in the Twentieth Century also brought a new age. From the middle ages to modern times, markets existed within the boundaries of regulated territories, and as info-communications technology developed and expanded the range of potential information sharing, those territories also expanded until, by the beginning of the Twentieth Century, almost every country had developed into a single market. It could be said that the legal framework of today's markets generally assumes a "one-country, one-market" situation. For example, the idea of banning the arbitrary or discriminatory provision of information in markets where this information should be shared is the basis of legislative regulation designed to preserve the efficiency of markets; however, this regulatory framework is built on the idea of the country as a unit.

In fact, this assumption of "one-country, one-market" was challenged by the development of the info-communications network in the 1980s. Giant leaps forward in the exchange and sharing of information across national borders through info-communications networks have expanded the breadth of the market, which up until now has existed as distinct individual systems in different countries. This is already giving birth to a large global market which transcends the country as a unit. This trend is particularly notable in industries such as the financial and telecommunications industries, in which restrictions on the delivery of the product are light. These industries have never before conducted business without considering the trends in foreign markets, and if laws and regulations are made without concern for conformity with systems used elsewhere, this would result in an immediate exodus of trade and wealth to other countries. In other words, in the end the continued expansion of markets in tandem with the development of info-communications technology crosses over national borders and brings about a phenomenon which should be called the superiority of the market over regulation by national agencies. Countries could also be said to be “kissing up” to the markets—a complete reversal of roles considering that countries used to rule the markets absolutely, before the markets outgrew the spatial bounds of countries where they had been under national rule since the Industrial Revolution.

To what degree should our legal system govern this global market? Many people believe that the watchword here should be “internationalization.” However, if by this term they mean more negotiation and coordination between governments representing the interests of their citizens, this term is at best insufficient, and perhaps not even necessarily correct. In the “one-country, one-market” era, negotiation and coordination between governments as the representatives of their respective markets was significant and necessary. However, the government’s position in a global market becomes somewhat more delicate and complex. In this situation, the government cannot help vacillating between the role of an overly strict supervisor, who may drive wealth out of the market, and that of an overly permissive guardian, who may create confusion.

Until now, the problems created by private law—particularly trade law—in international relations have been considered and argued in terms of conflict created at the point of contact between different jurisdictions. Certainly different markets have different information and customers and different legal procedures. In other words, the existence of many laws from many countries under the Nineteenth-Century “one-country, one-market” system is the root cause of the conflict between laws and the problem of coordinating those laws. However, as info-communications technology helps markets to exceed their national boundaries and create a “one-world, one-market” system, the conflict of laws will quickly escalate to a competition of laws. This is because, while global market transactions may contribute to dramatic expansion, they will also increase the severity of competition between the countries which provide the legal foundation for these transactions.

Generally speaking, some nations have industries whose raw materials are not easily moved across national borders, and their governments are quick to regulate and protect these industries. This is to their advantage because it helps maintain tax revenues and employment. Thus, the framework for international discussion about these industries seeks to prevent countries with conflicting interests from falling into competition and excessive regulation and taxation. The framework for GATT and WTO negotiations was based on doing away with tariff increases and non-tariff barriers, which is natural given the above context.

However, competition between countries with conflicting interests in information services, finance, electronic transactions, and similar new industries will result in the so-called race to the bottom, in which each country tries to attract these easily relocated industries with limited regulation and lower taxes. This competition may be an excellent microeconomic policy that brings to a country tax revenues and employment that would otherwise move elsewhere, but in a macroeconomic sense, it raises the potential for creating uneven distribution of resources in the world, resulting in unemployment and undue economic risks. The collapse of the stock market brought about by Enron's bankruptcy—a classic example of corporate corruption—is not only a failure of the market-monitoring mechanism, but also a demonstration of the propensity for risk brought about by computerization and competition of laws.

Cyber-Terrorism?

The terrorist attacks on 11 September 2001 gave rise to a wide range of discussion on terrorism. One of the subjects that occasionally arose was cyber-terrorism. However, the meaning of the term “cyber-terrorism” is not always clear. Some people use this word to mean the use of info-communications technology in destroying things, killing people, and other terrorist activities, while others use it to mean destructive actions targeting the info-communications system itself.

Naturally, with the spread of info-communications technology in society, it is taken for granted that both legal and illegal organizations make use of the info-communications system. Thus, we should be concerned about the potential of info-communications technology to affect the balance of power between those who would perpetrate crimes and those who would stop them, not only in relation to terrorism, but also to drug-dealing, kidnapping, and other common crimes.

Encryption technology is part of the technological infrastructure of open info-communications networks. This technology functions by creating a large discrepancy, in the volume of data processing required, between those who are trying to protect information and those who are trying to decrypt it. However, the declining price of (and remarkable increase in) CPU capacity in the 1990s made encryption technology relatively cheap to use. While this change enabled a wealth of possibilities for people using the Internet, it also provided a foundation for the activities of criminal organizations and anti-government organizations. Law enforcement agencies are therefore justified in their concern about the development and use of encryption technology. Yet, we should also keep in mind that the research, development, and private use of encryption technology should not be regulated. In contrast to nuclear and biological weapons, encryption development and research only requires a standard PC, paper, and pencil, and regulations would only prevent the use of information technology without contributing to the security of society. People using encryption technology in illegal activities will simply ignore the regulations and work at developing the technology, and it would be impossible to uncover all violations.

What in fact was the original context in which the phrase “cyber-terrorism” was used, and did such a phenomenon exist in that context? We must consider these questions calmly and carefully.

Terrorism generally occurs when the individuals in a group, small by comparison with society, feel an unusually strong animosity towards something, so much so that they are willing to sacrifice their lives to oppose it. However, the weakness of today’s network information systems is not demonstrated by a small number of groups which harbor extreme hostility, but by a great number of people who may feel slight displeasure on a whim.

No matter how much hatred and hostility there is towards a certain company or government, suicide bombing is not going to stop their activities on information networks. However, if a large number of people are displeased with a site (or with the company or government backing that site), even if their feelings are not that deep, they can easily shut down the site using a DoS (denial of service) attack. This is not a serious problem if the targeted site is only providing publicity or advertising. However, if the site is a commercial site, or one that provides medical histories, blood types, or other medical information, the attack will create a huge financial loss for the company. Yet, this possibility requires remedies which are vastly different from the physical and bodily countermeasures which are used to combat terrorism. The analogy between the use of computers to track down criminal computer activity on the Internet and the employment of physical and bodily countermeasures against terrorism is an over-simplification and prevents accurate estimation of the risks involved.