Cyber Crime . . . and Punishment?
Archaic Laws Threaten Global Information

December 2000

A Report Prepared By

McConnell International

www.mcconnellinternational.com

with support from

WITSA
World Information Technology and Services Alliance

www.witsa.org

CYBER CRIME . . . AND PUNISHMENT?
ARCHAIC LAWS THREATEN GLOBAL INFORMATION
DECEMBER 2000

Overview

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this report. Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

This report analyzes the state of the law in 52 countries. It finds that only ten of these nations have amended their laws to cover more than half of the kinds of crimes that need to be addressed. While many of the others have initiatives underway, it is clear that a great deal of additional work is needed before organizations and individuals can be confident that cyber criminals will think twice before attacking valued systems and information.

What's Different About Cyber Crime?

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency. According to the Computer Emergency Response Team Coordination Center (CERT/CC), the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54 percent over the total number of reported incidences in 1999.[1] Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities, the potential for copycat crimes, and the loss of public confidence.

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require

[1] See www.cert.org. Although the following organizations also track reported incidents, global statistics have yet to be compiled: the National Infrastructure Protection Center (NIPC), www.nipc.gov, the Computer Security Institute (CSI), www.gocsi.com, and the Internet Fraud Complaint Center, www.ifccfbi.gov.

few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

As this report shows, the laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks[2] may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billions of dollars of damage worldwide.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

Six weeks after the Love Bug attack, the Philippines outlawed most computer crimes as part of a comprehensive e-commerce statute. In order to prevent a repeat of the catastrophe that prompted this action, however, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise enforceable laws that will effectively deter all but the most determined cyber criminals.

Poor Information Security Reduces the Competitiveness of Nations

In our August 2000 report, *Risk E-Business: Seizing the Opportunity of Global E-Readiness,* McConnell International rated mid-level economies' capacity to participate in the digital economy.[3] In considering nations' information security, the report evaluated public trust in the security of information processed and stored on networks in each country. In this context, information security included: an assessment of the strength of legal protections and progress in protecting intellectual property rights, especially for software; the extent of efforts to protect electronic privacy; and the strength and effectiveness of the legal framework to authorize digital signatures. The E-Readiness report also examined the existence of legal frameworks to prosecute cyber criminals, for a predictable environment of strong deterrence for computer crime is critical to the effective protection of valuable information and networks.

Although several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors, few countries were able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of cyber crime would be held accountable for their actions. Overall, nearly half of the countries included

[2] Victims of recent attacks include: Yahoo, CNN Interactive, Amazon.com, eBay, Datek Online, E*Trade, ZDNet, and Buy.com.

[3] The report evaluated nations' Connectivity, E-Leadership, Information Security, Human Capital, and E-Business Climate. This report is available at www.mcconnellinternational.com/ereadiness/report.cfm.

in the E-Readiness study were rated as needing substantial improvement in information security. In addition, only a small fraction of countries needing substantial improvement indicated that progress was currently underway.

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce. As e-business expands globally, the need for strong and consistent means to protect networked information will grow.

The Cyber Crime Laws of Nations

Based on its findings in the E-Readiness study, and in the wake of the Philippines inability to prosecute the student responsible for the "I Love You" virus, McConnell International surveyed its global network of information technology policy officials to determine the state of cyber security laws around the world. Countries were asked to provide laws that would be used to prosecute criminal acts involving both private and public sector computers.

Over fifty national governments[4] responded with recent pieces of legislation, copies of updated statutes, draft legislation, or statements that no concrete course of action has been planned to respond to a cyber attack on the public or private sector. Countries were provided the opportunity to review the presentation of the results in draft, and this report reflects their comments.

Countries that provided legislation were evaluated to determine whether their criminal statutes had been extended into cyberspace to cover ten different types of cyber crime in four categories: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including aiding and abetting cyber criminals, computer fraud, and computer forgery.

Thirty-three of the countries surveyed have not yet updated their laws to address any type of cyber crime. Of the remaining countries, nine have enacted legislation to address five or fewer types of cyber crime, and ten have updated their laws to prosecute against six or more of the ten types of cyber crime.

Figure 1 provides a categorization of the 52 countries surveyed.

[4] The countries evaluated are: Albania, Australia, Brazil, Bulgaria, Burundi, Canada, Chile, China, Cuba, the Czech Republic, Denmark, Dominican Republic, Egypt, Estonia, Ethiopia, Fiji, France, Gambia, Hungary, Iceland, India, Iran, Italy, Japan, Jordan, Kazakhstan, Latvia, Lebanon, Lesotho, Malaysia, Malta, Mauritius, Moldova, Morocco, New Zealand, Nicaragua, Nigeria, Norway, Peru, Philippines, Poland, Romania, South Africa, Spain, Sudan, Turkey, United Kingdom, United States, Vietnam, Yugoslavia, Zambia, and Zimbabwe.

Figure 1: Extent of Progress on Updating Cyber Crime Laws

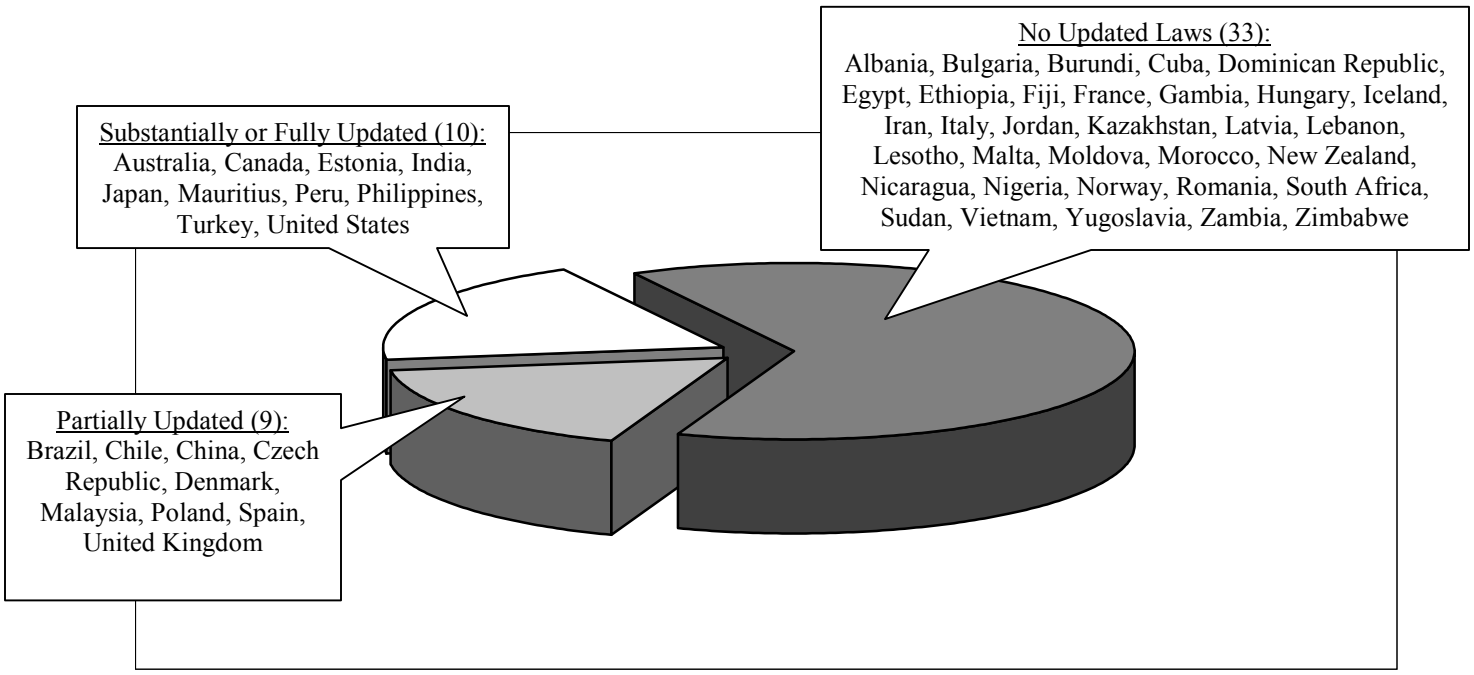

Figure 2 details which laws have been updated in each of the 19 countries with fully, substantially, or partially updated laws in place. Excerpts from, or the full text of, pertinent statutes are available on the McConnell International website, www.mcconnellinternational.com, for each of the countries in Figure 2. In Canada, successful prosecutions of computer-related fraud have effectively updated the law. Canada also provides an example of a phenomenon in many countries—that law enforcement officials have strong confidence that existing laws provide sufficient coverage against the "computer-related crimes" of aiding and abetting cyber crimes, and computer-related fraud and forgery.

Even among these countries, crimes are not treated uniformly. In some, unauthorized access is a crime only if harmful intent is present; in others, data theft is a crime only if the data relates specifically to an individual's religion or health, or if the intent is to defraud. Laws tend to be biased in favor of protecting public sector computers. Many of the laws reviewed in preparing Figure 2 outlaw crimes committed with or against government computers, but do not provide reciprocal protection to private sector computers.

Discrepancies exist even within countries. For example, in September 2000, the Australian Democratic Party criticized the South Australian (state) government for creating a haven for cyber criminals by not having updated its laws to combat computer-based crime in accordance with the laws of Australia's other states. Moreover, as Figure 2 shows, there is little uniformity across nations in terms of which types of crimes have been addressed through updated statutes.

The penalties provided in updated criminal statutes vary widely. Mauritius, the Philippines, and the United States have stronger penalties than many other countries for convictions of covered cyber crimes.

Figure 2: Countries with Updated Laws										
Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Republic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Mauritius	✔	✔		✔	✔	✔	✔	✔	✔	
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

Key for Figure 2

Data Interception: Interception of data in transmission.
Data Modification: Alteration, destruction, or erasing of data.
Data Theft: Taking or copying data, regardless of whether it is protected by other laws, e.g., copyright, privacy, etc.
Network Interference: Impeding or preventing access for others. The most common example of this action is instigating a distributed denial of service (DDOS) attack, flooding Web sites or Internet Service Providers. DDOS attacks are often launched from numerous computers that have been hacked to obey commands of the perpetrator.
Network Sabotage: Modification or destruction of a network or system.
Unauthorized Access: Hacking or cracking to gain access to a system or data.
Virus Dissemination: Introduction of software damaging to systems or data.
Aiding and Abetting: Enabling the commission of a cyber crime.
Computer-Related Forgery: Alteration of data with intent to represent as authentic.
Computer-Related Fraud: Alteration of data with intent to derive economic benefit from its misrepresentation.

Finally, of the 33 countries with no updated laws in place, 13 indicated that progress toward the adoption of updated legislation to combat cyber crime is underway. Seven of these 13 countries are in Africa or the Middle East, indicating that, although these regions have not yet adequately addressed the issue of cyber crime, many countries are aware that action is needed. Figure 3 offers a summary of work in progress.

Figure 3: Progress Underway in 13 Countries Without Updated Laws

Albania	The Authority for the Regulation of Telecommunications began discussions earlier this year on the topic of cyber laws, with the goal of preparing protocols of collaboration and exchanging information.
Cuba*	A working group of the Ministry of Justice has planned modifications to the Penal Code.
Gambia	Gambia is planning a national information technology initiative, although the capacity for the drawing up a legal framework is limited. Gambia may look towards international organizations to spearhead this effort so that it could replicate or amend the needed laws.
Iran	For the past six years, Iran has examined various aspects of cyber law, although no law or regulation in regard to computer offenses has been implemented. The areas that have been considered are: computer offenses, intellectual property issues, privacy/data protection, and freedom of information.
Kazakhstan	State bodies in Kazakhstan are currently developing a law regarding cyber offences. Also in development is a special state program on the protection of information resources, including technical and software protection.
Latvia*	Amendments to the Criminal Code have been drafted envisaging considerable punishment for computer-related criminal acts. Corresponding additions would be made to the Administrative Offence Code.
Lesotho	Lesotho has established special interest groups to look at the various aspects of information security relating to e-commerce.
Malta*	In May 2000, Malta announced its goal of providing a strong legal framework for e-commerce, data protection, and computer misuse. The relevant Bills to develop a legislative framework for information practices were published in September 2000 and will be discussed in parliament in the coming months.
Morocco	In Morocco, there is an inter-ministerial commission sponsored by the Prime Minister working on security issues.
New Zealand*	At present there are no general computer crime offences in New Zealand. However, the country is currently drafting a Crimes Amendment Bill (No. 6).
Sudan	The Sudan intends to invite lawyers, legislators and computer professionals to a workshop where ideas on the nature of computer crimes and the ways of dealing with them by means of the appropriate legal codes will be exchanged.
Vietnam	Vietnam is in the process of gathering information to make proposals for amendments to its laws.
Zambia*	Zambia has made available a draft of its Telecommunications and Information Technology Council Act.

* Copies of relevant drafts are available at www.mcconnellinternational.com.

Law Is Only Part of the Answer

Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and businesses. Because that extension remains a work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide.

To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process, and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology--such as firewalls, anti-virus software, intrusion detection tools, and authentication services--throughout the organizations' computer systems.

These system protection tools--the software and hardware for defending information systems--are complex and expensive to operate. To avoid hassles and expense, system manufacturers and system operators routinely leave security features "turned off," needlessly increasing the vulnerability of the information on the systems. Bugs and security holes with known fixes are routinely left uncorrected. Further, no agreed-upon standards exist to benchmark the quality of the tools, and no accepted methodology exists for organizations to determine how much investment in security is enough. The inability to quantify the costs and benefits of information security investments leave security managers at a disadvantage when competing for organizational resources. Much work remains to improve management and technical solutions for information protection.

Industry-wide efforts are underway to address prevention, response, and cooperation. Around the world, various industries have been establishing information sharing and analysis centers (ISACs) to share real-time information related to threats, vulnerabilities, attacks, and countermeasures. A recent Global Information Security Summit sponsored by the World Information Technology and Services Alliance (www.witsa.org) brought together industry, governments, and multilateral organizations across economic sectors to share information and build partnerships. Post-summit working groups are now developing cooperative approaches to addressing the most critical information security problems. The results of that work will be taken up at a second summit in Belfast in May 2001. That summit will also provide an opportunity to revisit the progress of nations in updating their laws to cover cyber crimes.

Conclusions

1. Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

2. Weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

3. Self-protection remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

4. A global patchwork of laws creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. Figure 2 illustrates the kinds of gaps that remain, even in the 19 countries that have already taken steps to address cyber crimes. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated.

5. A model approach is needed. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

Recommendations

The weak state of global legal protections against cyber crime suggests three kinds of action.

1. Firms should secure their networked information.

Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

2. Governments should assure that their laws apply to cyber crimes.

National governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.

3. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security.

To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe (see www.coe.int), comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data. Finally, it promotes cooperation among law enforcement officials across national borders.

Late in its process, the Council began to consider the views of affected industry and civil society. This process is making the Council's product more realistic, practical, efficient, balanced, and respectful of due process that protects individual rights. At this point, most observers support provisions to improve law enforcement cooperation across borders. However, industry, through the World Information Technology and Services Alliance (see www.witsa.org/press/), argues that the requirements on service providers to monitor communications and to provide assistance to investigators, as outlined in the Draft Convention, would be unduly burdensome and expensive. Another provision considered objectionable could criminalize the creation and use of intrusive software, or hacking programs, which are designed for legitimate security testing purposes. This action could stifle the advances in technology vital to keep up with evolving cyber threats. Privacy and human rights advocates (see www.gilc.org) object to the Draft Convention's lack of procedural safeguards and due process to protect the rights of individuals, and to the possibility that the ensuing national laws would effectively place restrictions on privacy, anonymity, and encryption.

The Council plans to release a final draft of the Convention in December 2000. In 2001, a political process involving national governments will determine the scope and coverage of the final Convention. Because of cyber crime's international potential, all countries, and all companies, are affected. Interested parties, including national governments from outside Europe, and businesses and non-governmental organizations from around the world, should participate vigorously in a consensus process to develop measures that support effective international law enforcement and foster continued growth and innovation.

What is McConnell International?
McConnell International (MI) is a global technology policy and management consulting firm that helps clients seize opportunities in the new economy. Its proven approach of using trusted public and private networks to leverage the risk of e-business and e-government gives clients a unique advantage. MI currently manages the United Nations-sponsored global cooperation network of government Internet policy officials from over 120 countries.

What is the MI Mission?
The mission of McConnell International is E-Readiness impact. Achieving high levels of E-Readiness enables our clients to become global leaders in electronic business and government.

What Does MI Do?
McConnell International positions its corporate and government clients to take maximum advantage of the new economy by finding solutions at the intersection of business, governance, and technology. MI serves its clients through:

- Strategic Advice. Apply the most current knowledge available on changing e-business and e-government conditions worldwide to design projects and implement strategies that benefit from these changes.

- Building Partnerships and Opening Doors. Identify partners for information and communication technology projects and help businesses and governments build alliances.

- International Visibility. Promote your business or government as an innovator and leader in the new economy.

- Research and Analysis. Make sound decisions and advocate for positive change based on MI's in-depth knowledge and published scorecards on the networked world, including an August 2000 report on E-Readiness and a December 2000 Cyber Crime report. A second report on E-Readiness will be published in March 2001.

- Project Design. Identify and initiate ventures in new and existing markets, yielding more customers, stronger partners, and increased revenues.

How Is MI Unique?
MI has a world-class track record solving tough international technology management problems for large organizations and is recognized by the global media as experts on e-business climate. MI distinguishes itself by:

- Focusing solely on e-business and e-government.
- Operating a worldwide government-to-government Internet policy network.
- Its energy, agility, and appreciation of the absurd.
- The experience of Bruce McConnell and Roslyn Docktor, who led the International Y2K Cooperation Center.

1341 G Street, NW - Suite 1100
Washington, DC 20005

[1] 202-347-7445 fax 347-7446
info@mcconnellinternational.com