Articles

The Scope and the Nature of Computer Crimes Statutes - A Critical Comparative Study

Rizgar Mohammed Kadir [*]

Abstract

When computer crime statutes had yet to be enacted, computer crimes were subjected to traditional criminal laws. This policy resulted in greater expense and other considerable difficulties. These problems and difficulties paved the way for the emergence of a consensus calling for legislators to intervene and enact specific computer crime legislation suited to confronting this new type of criminal activity. Many countries in the world responded by enacting new criminal legislation and many others are on their way to take similar legislative steps.

For the legislative intervention to be sound and successful two major questions should be adequately addressed; the scope of legislative intervention and the nature of computer crime legislation enacted. Regarding the first question, new criminal provisions are needed only to cover those crimes that are unique to computers themselves, other crimes in which a computer is used simply as an instrument for perpetration are either covered by existing criminal provisions or can be covered by simple amendments of said provisions. Another step that should be taken by legislators is the amendment of existing criminal laws with an aim to cover some special cases such as the cases in which the computer is used as an instrument for committing known traditional crimes, making the perpetration of such crimes easier or resulting in more dangerous consequences compared to their more traditional forms and cases in which intangible digitized property comes under threat from criminal activities.

While many countries in the world have soundly followed such a method in dealing with computer related misconducts legislatively, others have failed to do so. In some countries, the legislator has criminalized some criminal conducts that have long since been criminalized by that country's penal code. This creates conflict between criminal provisions, posing problems to prosecutors and courts alike.

Regarding the nature of computer crime statutes, the legislator is presented with two options. The first is the inclusion of the aforementioned criminal provisions in one separate

[*] Assistant Professor of Criminal Law, College of Law and Politics – Department of Law, Salahaddin University, Erbil - Kurdistan Region, Iraq. Email: rizgar70m@yahoo.com.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

code as one specific computer crime statute. The second is inserting substantive criminal provisions related to computer crimes into the existing penal law of the country. While the first method preserves the unity of substantive criminal law of the country in one code and prevents the dispersion of criminal provisions into many separate laws, the second one would, by contrast, create much-needed public awareness of computer crime.

A. Introduction

Criminal law plays a prominent role in the life of society and performs several functions: deterring people from committing acts that harm others or society; determining the conditions under which people who have performed such acts will be punished; and providing some guidance on the kinds of behavior that are regarded by society as acceptable.[1]

Since one of the main functions of the criminal law is to determine which human conducts are regarded as crimes, and given that the advance of society might bring new harmful conducts, the list of conducts prohibited and punished by the legislator through the criminal law is neither fixed nor unchanged forever. Although almost all nations in the world have recognized many forms of conduct, such as murder or theft, as crimes since antiquity, the forms of conduct criminalized by a given criminal law of a certain country are not exactly the same as those criminalized by the criminal law of the same country fifty years ago.

For the facts and reasons mentioned above, the legislator is always obliged to review the criminal law from time to time whenever a new type of harmful conducts emerges. This was exactly what happened when computers entered the lives of individuals and societies. Although the new technology provided many new benefits, it led, at the same time, to the emergence of new criminal activities and enhanced the capabilities of criminals to a great extent.[2]

With the emergence of *Computer Misuse Act*ivities, a consensus that such activities must be prevented and punished emerged. As a result of this, a crucial question arose concerning the best legislative way of accomplishing this[3]. While many scholars saw that

[1] Jonathan Herring, Criminal Law 4-5 (2002).

[2] Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to A Growing Problem, 43 Vanderbilt Law Review (Vand. L. Rev.) 453 (1990), 454.

[3] Amalia M. Wagner, The Challenge of Computer – Crime legislation: How Should New York Respond, 33 Buffalo Law Review (Buff L. Rev.) 777 (1984), 795.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

the traditional existing criminal statutes were sufficient for successfully prosecuting any type of computer abuses, many others presented strong legal, technical and practical arguments, and strongly believed that the existing criminal statutes were not suitable for the digital era; the nature of computer crime necessitates specialized legislation.[4] However, this dispute did not last long and was settled in favor of those demanding legislative action. Consequently, many countries around the world began to enact new legislation addressing criminal activities brought by computer technology ('computer crimes').

This Article will deal with the question of computer crime statutes: how they should be designed and what they should include? Here, the aim of this study becomes apparent; it intends to seek out the soundest method to be followed in formulating computer crimes statues. To achieve this goal, we are going to shed light on computer crimes in Section B of this Article. Awareness of their types and natures is an indispensable step towards determining the sound legal treatment of such crimes. Section C of this Article will be devoted to computer crimes statutes. We will discuss the basic characteristics of such statutes and how the legislator must deal with computer crimes legislatively. The focus of Section D will be on the offences that are unique to the computer, as these should be the subject of the legislator's attention. Given that this study is a comparative one, it examines the experiments of many countries that have dealt with the question of computer crimes legislatively, particularly those of European nations. The study of the European experiments will include both national and collective efforts in dealing with the problem.

B. Understanding Computer Crime

In this Section we will shed light on some general aspects of computer crimes[5], as these clarifications are necessary for a sound understanding of computer crimes. These include the definitions of computer crimes, their types and categories and the computer criminals themselves. Each of these subjects will be treated in separate subsections.

[4] Douglas H. Hancock, To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention?, 12 Albany Law Journal of Science & Technology (Alb. L.J. Sci. & Tech.) 97 (2001), 97; Carla Ottaviano, Computer Crime, 26 IDEA: The Journal of Law and Technology (IDEA) 163 (1985-1986), 167.

[5] At present, several terms are used for naming misconducts relating computer and Internet including 'cybercrime', 'e-crime', 'digital crime' etc. See, RUSSEL G. SMITH ET AL, CYBER CRIMINALS ON TRIAL 5 (2004). For the purpose of this Article, I will mainly use the term 'computer crime'.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

I. Defining Computer Crimes

The definition of any subject matter is an indispensable step towards any proper legal treatment of that subject. However, the problem of properly identifying and defining a crime presents itself each time a new field of law emerges.[6] When academics first began to discuss the question of computer misuses, they soon found themselves face to face with this problem. As the United Nations Manual on the Prevention and Control of Computer Crime has prescribed, "[t]here has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime. Even after several years, there is no internationally recognized definition of those terms."[7]

In 1989, expanding on work undertaken by the Organization for Economic Co-operation and Development (OECD), the European Committee on Crime Problems of the Council of Europe laid down a body of guidelines for national legislators concerning activities that should be criminalized. The Committee, however, simply discussed the functional characteristics of target activities without providing a formal definition of computer crime, allowing individual countries to adapt the functional classification to their particular legal systems and historical traditions.[8]

Agreement upon a uniform definition of computer crime is helpful for both law enforcement and industry alike.[9] The results of a survey sent to several state prosecutors in the United States on the subject of computer crime indicated significant disparities in terms of what constitutes computer crime.[10]

These disparities appear to arise for several reasons. Foremost is the absence of an agreed upon definition of the 'computer', a definitional problem at the forefront of legal scholars' search for a proper definition of computer crime. When the United States Congress passed

[6] See, *supra,* note 3, 782.

[7] UNITED NATIONS COMMISSION ON CRIME PREVENTION AND CRIMINAL JUSTICE, INTERNATIONAL REVIEW OF CRIMINAL POLICY – UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER CRIME. , 8th Cong. 21 (Vienna, April 27 – May 6, 1999), available at: http://www.uncjin.org/Documents/irpc4344.pdf (last accessed 12 June 2010).

[8] *Id*, 23.

[9] Carol C. McCall, *Computer Crime Statutes: Are They Bringing the Gap between Law and Technology*, 11 CRIMINAL JUSTICE JOURNAL (CRIM. JUST. J.) 203 (1988-1989), 208.

[10] *Id*, 208-9, citing D. PARKER, FIGHTING COMPUTER CRIME (1988), 236-44 (1988).

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

the first piece of federal legislation focusing directly on computer abuses[11], it defined a 'computer' as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."[12] The definition, however, has been criticized by some computer experts in that "[t]his limited definition fails to recognize the substantial changes in technology that have evolved from main-frame to hand-held computers."[13] The United Kingdom legislation, the *Computer Misuse Act* 1990[14], failed to define a 'computer' at all; the Law Commission stated that "all the attempted definitions that we have seen are so complex, in an endeavor to be all-embracing, that they are likely to produce extensive arguments, and thus confusion for magistrates, juries and judges involved in trying our proposed offences."[15]

Another factor might be the lack of comprehensive knowledge about the problem together with the legal and technical dimensions necessary to establish a proper definition. One commentator has aptly described this problem as such: "[c]omputer crime was analogous to the proverbial emperor's clothes: everybody proclaimed it was there, but no one could see it. The little extant data established that some sort of problem existed, but no one had a clear idea of its nature or extent."[16]

Some legal scholars have attempted to avoid a precise definition. In lieu of providing even a general definition, they have instead depended on referring as much as possible to the misuses attached to the computer and Internet. One such scholar writes: "[t]his umbrella

---

[11] *Counterfeit Access Device and Computer Fraud and Abuse Act of 1984*, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. section 1030 (1988)).

[12] *Id*, section 1030(e).

[13]See, *supra,* note 9, 208 citing D. PARKER, FIGHTING COMPUTER CRIME 242 (1988). See, however, *supra,* note 2, 461: "[t]he adopted definition of 'computer'' was intended to limit the type of activity prohibited under the 1984 Act by explicitly excluding automated typewriters, typesetters, hand held calculators, and other similar devices. This exclusion helped to ensure that the legislation did not prohibit conduct which Congress did not intend to proscribe."

[14] *Computer Misuse Act* (1990), ch. 18, the full text of it is available at: http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (last accessed 14 June 2010).

[15] Steve Shackelford, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEXAS INTERNATIONAL LAW JOURNAL (TEX. INT'L L.J.) 479 (1992), 491 (citing The Law Commission, Working Paper No. 186, Criminal Law Computer Misuse 23 (1989)).

[16] See, *supra,* note 2, 483.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

term covers all sorts of crimes committed with computers - from viruses to Trojan horses; from hacking into private e-mail to undermining defense and intelligence systems; from electronic thefts of bank accounts to disrupting web sites".[17] In a similar vein, another commentator notes that "[i]n general, computer crime consists of volitional, nonviolent acts involving a computer".[18] Yet another claims that the term 'computer crime' "usually means nothing more than the use of a computer to embezzle or steal money or other property".[19]

Other legal scholars have argued that a broad definition should be adopted: "because of the diversity of computer related offences, a narrower definition would not be adequate. While the term 'computer crime' includes traditional crimes committed with the use of a computer, the rapid emergence of computer technologies and the exponential expansion of the Internet have spawned a variety of new, technology-specific criminal behaviors that must also be included in the category of computer crimes."[20]

The United States Department of Justice has defined computer crime as "any violation of criminal law that involves a knowledge of computer technology for their perpetration, investigation, or prosecution."[21] Of course, this definition is a broad one; it is indeed derived from the definition provided by Parker and Nycum, the authors of the first comprehensive study on the computer crime in 1979. According to them, computer crime is "any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution."[22] Other later and more obscure definitions are basically dependent on this seminal definition.[23] However, the definition introduced by J.

---

[17] Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (U. PA. L. REV.) 1003 (2001), 1004.

[18] Robert M. Couch, *A Suggested Legislative Approach to the Problem of Computer Crime*, 38 WASHINGTON AND LEE LAW REVIEW (WASH. & LEE L. REV.) 1194 (1981), 1175.

[19] Gary J. Valeriano, *Pitfalls in Insurance Coverage for "Computer Crimes"*, 59 DEFENSE COUNSEL JOURNAL (DEF. COUNS. J.) 511 (1992), 511.

[20] Robert Ditzion et al., *Computer Crimes*, 40 AMERICAN CRIMINAL LAW REVIEW (AM. CRIM. L. REV.)285 (2003), 286.

[21] Julie A. Tower, *Hacking Vermont's Computer Crimes Statute*, 25 VERMONT LAW REVIEW 945 (2001), 950 (citing National Institute of Justice, U.S. Department of Justice, Computer Crime: Criminal Justice Resource Manual 2 (1989)).

[22] See, *supra,* note 9, 208 citing S. NYCUM & D. PARKER, PROSECUTORIAL EXPERIENCE WITH STATE COMPUTER CRIME LAWS 34 (1986).

[23] See, Jo-Ann M. Adams, Comment, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECHNOLOGY LAW JOURNAL (SANTA CLARA COMPUTER & HIGH TECH L.J.) 403 (1996), 409 (defining computer crime as "those crimes where knowledge of a computer system is essential to commit the crime"); Barry J. Hurewitz & Allen M. Lo, *Computer-Related Crimes*, 30 AMERICAN CRIMINAL LAW REVIEW

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

Soma in 1983 might be seen as one that is more well-developed. According to Soma, computer crime is "the use of computer or its technology as a target of or a tool for illegal purposes".[24]

The existing computer crime legal literatures produced in the last three decades indicate that the general tendency, for both clarifying the meaning of computer crime on the one hand and determining the behaviors that constitute computer offences on the other, was, and still is, the dependence on the categorization of computer related misuses more so than any one specific definition. Precisely this predominant tendency will form the subject matter of the next subsection.

II. Types of Computer Crime

Determining the types of unacceptable activities related to the computer is relevant because, as will be seen in subsequent sections of this article, the quality of their legislative treatment can only be as good as the original determination and classification of such activities.

Abuses, misuses or crimes attached to computers take different and various forms. They are, however, classified in several ways and according to more than one criterion. One such classification makes use of two categories: (1) crimes where a computer system itself is the target such as hacking, dissemination of viruses, and denial of service attacks; (2) traditional crimes like fraud, theft, and child pornography that are facilitated and enabled by a computer.[25]

The second classification system categorizes computer crimes into four types; (1) theft of money, financial instruments, property, services, or valuable data; (2) unauthorized access to computer time; (3) illegal use of computer programs; and (4) unauthorized acquisition of stored data.[26]

(AM. CRIM. L. REV.) 495 (1993), 496 (defining computer crime as "any illegal act for which knowledge of computer technology is essential for prosecution").

[24] J. SOMA, COMPUTER TECHNOLOGY AND THE LAW 265 (1983). Cited by William S. Allred, *Criminal Law- Connecticut Adopts Comprehensive Computer Crime Legislation: Public Act 84-206*, 7 WESTERN NEW ENGLAND LAW REVIEW (W. NEW ENG. L. REV.) 807 (1984-1985), 810.

[25] Brian C. Lewis, *Prevention of Computer Crime Amidst International Anarchy*, AMERICAN CRIMINAL LAW REVIEW (AM. CRIM. L. REV.) 1353 (2004(, 1355 ("In general, computer crimes are crimes where a computer system itself is the target, while computer- enabled crime is a traditional crime like fraud or theft that is facilitated by a computer").

[26] Elizabeth A. Glynn, *Computer Abuse: The Emerging Crime and the Need for Legislation*, 12 FORDHAM URBAN LAW JOURNAL (FORDHAM URB. L.J.) 73 (1984), 74-5.

According to one commentator, there are four basic types of computer-related crimes: (1) theft of computer time and services; (2) theft of computer software or data; (3) theft of computer hardware, including components that may constitute trade secrets; and (4) theft of property by the use of a computer.[27]

Another classification system adopted by the United States Department of Justice seems to be particularly reliable and effective. This system separates computer crimes into three categories according to the computer's role in a particular crime; first, the computer may be the 'object' of a crime. This happens when the criminal launches an attack upon an individual computer or a network: "[s]uch attacks may include unauthorized access to information stored on the computer or the targeted network; the unauthorized corruption of that information; or theft of an electronic identity".[28] Second, the computer may be the 'subject' of a crime; this happens when the computer is "the physical site of the crime, or the source of, or reason for, unique forms of asset loss."[29] Hacking and dissemination of viruses, worms, logic bombs and Trojan horses are some of the more common threats posed when a computer is the subject of an attack.[30] Finally, a computer could be the instrument for perpetrating traditional offences. For example, a computer can be used to steal credit card information, store and distribute obscenity[31], or distribute child pornography and other types of obscene materials through computers linked to the Internet.[32] The computer can even be used as an instrument to commit traditional violent crimes such as homicide. In New Zealand, for example, two programmers were convicted in 1980 of involuntary manslaughter when they caused an airliner crash that resulted in 257 deaths through criminal negligence in programming flight navigation.[33]

[27] See, *supra,* note 19, 512.

[28] Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEORGE MASON LAW REVIEW (GEO. MASON L. REV.) 237 (2000), 243.

[29] Laura J. Nicholson et al, Comment, *Computer Crimes*, 37 AM. CRIM. L. REV. 207 (2000), 211.

[30] See, *supra,* note 28, 246-249.

[31] *Id.,* 242.

[32] *Id*., 249.

[33] See, *supra,* note 9, 204 citing *Causes of DC10 Crash on Erebus*, ANTARCTIC (June 1981), 186.

III. Computer Criminals

There is no 'typical' computer crime and no 'typical' motive for committing such crimes.[34] The UN Manual has indicated that computer criminals can vary in terms of both age and skill level.[35] They can be teenage hackers, disgruntled or fired employees, mischievous technicians, or international terrorists.[36] Some argue that computer offenders have morphed from mischievous, thrill-seeking teenagers to criminals intent on making large profits.[37] Regarding possible motives, one commentator has identified six motives for committing computer-related crimes where computers are subjects or objects of crime: (1) to exhibit technical prowess; (2) to highlight vulnerabilities in computer security systems; (3) to punish or retaliate; (4) to engage in computer voyeurism; (5) to assert a philosophy of open access to computer systems; and (6) to sabotage.[38]

Another topic of controversy is related to the typical skill level of the computer criminal; while some adhere to the opinion that skill level is not an indicator of a computer criminal, others believe that potential computer criminals are bright, eager, highly motivated subjects willing to challenge the technology.[39]

Although the types of crimes that are related to the computer in one way or another are limitless, the perpetrators of computer crime form two distinct classes: insiders and outsiders.[40] The insider is "anyone who has the same or similar access rights into a network, system, or application. Therefore, a trusted insider can be a current or former employee, a contractor, consultant, service provider, software vendor, and so on".[41] The

[34] Michael Hatcher, *Computer Crimes*, 36 AM. CRIM. L. REV. 397 (1999), 400.

[35] See, *supra,* note 7, 34.

[36] Adam G. Ciongoli, *Ninth Survey of White Collar Crime, Computer-Related Crimes*, 31 AM. CRIM. L. REV. 425 (1994), 427.

[37] Xan Raskin & Jeannie Schaldach-Paiva, *Eleventh Survey of White Collar Crime, Computer Crimes*, 33 AM. CRIM. L. REV. 541 (1996), n. 7 citing William C. Flanagan & Brigid McMenamin, *The Playground Bullies are Learning How to Type*, Forbes (Dec. 21, 1992), 184.

[38] Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL (RUTGERS COMPUTER & TECH. L.J.) 1 (1990), 24-26.

[39] See, *supra,* note 7, 33.

[40] See, *supra,* note 15, 482.

[41] KENNETH C. BRANCIK, INSIDER COMPUTER FRAUD: AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER ATTACKS 1, 4 (2008).

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

insider who threatens the company or the government agency is basically anyone who has access to high technology, intellectual property, and other sensitive information stored in high-technology equipments as well as input documents or output documents. They include, but are not limited to, auditors, security personnel, marketing personnel, accountants and financial personnel, managers, inventory and warehouse personnel, and human resource staff.[42]

By contrast, the list of outsider offenders includes hackers, vendors, ex-employees, employees of associated businesses, state sponsored such as foreign government agents, customers, subcontractors, terrorists, contractors, external auditors, consultants, political activists, criminals in general, pressure groups and commercial groups.[43]

In the earlier days of the computer and prior to the internet, insider computer crimes predominated and perpetrators were generally computer specialists: programmers, computer operators, data entry personnel, systems analysts, and computer managers.[44] The advent of the Internet, however, soon made it possible to commit such crimes from outside a victimized computer. However, insider abuses of network access by employees still far outnumber abuses perpetrated by the outsider;[45] one study indicates that 90 per cent of economic computer crimes are committed by employees of the victimized company. A recent survey in North America and Europe indicated that 73 per cent computer security risks are from internal sources and only 23 per cent can be traced to external criminal activities.[46] Some commentators, however, argue that the split is more even, ranging around 50 per cent for each: "[w]ith the integration of telecommunications and computers, along with the integration of government agencies and businesses into the Internet, threats now represent at least an equal split between internal and external threat agents—50% internal and 50% external. There may even be a slight edge toward external threat agents because of today's reliance on the Internet and other corporate and externally connected networks".[47]

---

[42] GERALD L. KOVACICH & ANDY JONES, HIGH TECHNOLOGY CRIME INVESTIGATOR'S HANDBOOK 28, 9 (2006).

[43] *Id.*, 31 (indicating that outsiders share the same motivations as insiders in addition to the following motivations: revenge of a former employee, competitors wanting inside information, new employees who provide information relative to their previous employer, former employee curiosity about their previous access ID and password still being valid, political agenda, environmental activists attacking corporations who they believe are harming the environment, nationalistic economic pressures, espionage and information warfare). *Id.*, 32.

[44] *Id.*, 24.

[45] See, BERNADETTE H. SCHNELL & CLEMENS MARTIN, CYBERCRIME – A REFERENCE HANDBOOK XII (2004)

[46] See, *supra,* note 7, 35.

[47] See, *supra,* note 42, 26.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

As one commentator has pointed out, the insider/outsider distinction is relevant because the method of entry followed by the person and type of misuse will often determine whether the law will come into play. For example, an insider who is an accountant with high-level computer access can embezzle funds from his company more easily than an outsider.[48] Because insiders have physical access, they can copy data to removable media or to a portable computer, or perhaps even print it to paper and remove it from the premises. They can change the format of the data to disguise it.[49] These capabilities are not available to an outsider. An outsider may gain access to the system, but only in an unauthorized manner; he will draw attention to himself more quickly than will the insider.[50]

To this we can add another legal consequence of the insider/outsider distinction. The traditional criminal laws always deal more severely with those who are on the same or similar footing as the insider in the realm of computer and electronic networks. Thus, criminal recognition of insider crime is nothing new; the traditional criminal law regarded it as an aggravating circumstance even before the emergence of insider computer and Internet offences. This is reflected in some of the offences recognized in some traditional criminal law systems. For example, facilitating escape of prisoners' in German Criminal Law is imprisonment of not more than three years or a fine, but if the offender is under duty as a public official or a person entrusted with special public service functions to prevent the escape of the prisoner, the penalty shall be imprisonment of not more than five years or a fine.[51] Another example can be seen in the treatment of theft in *Iraqi Penal Code*; if the person perpetrating the offence is the servant of the master against whom the crime is committed, he will receive a more severe punishment than what he might receive if he was not a servant. The same rule applies to a worker in a factory, shop or a place where she normally works.[52] In light of these facts, when the legislator begins to lay down punishments for different types of computer abuses, it is necessary to regard any insider crime as an aggravating circumstance deserving a more severe punishment.

[48] See, *supra,* note 15, 482.

[49] DEBRA LITTLEJOHN SHINDER, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 289 (2002).

[50] See, *supra,* note 15, 482.

[51] See, *German Criminal Law* (*StGB*), Section 120.

[52] See, *Iraqi Penal Code* (1969), article 444(6).

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

C. Computer Crimes Statutes

Prior to the existence of computer crime statutes, traditional criminal laws were manipulated to accommodate new technology. Applying traditional criminal law to computer crime resulted in greater expense in the prosecution of offences only remotely related to the real nature of the acts committed[53], and prosecutors faced difficulties in submitting computer related misconducts to traditional criminal provisions.[54] These problems and difficulties led to a consensus on the need for legislative intervention providing specific computer crimes legislation suited to confronting this new type of criminal activity.[55] At this point, the crucial questions revolved around the scope of such intervention on the one hand, and the nature of such computer crimes legislation on the other.[56] These questions will be subjected to a more detailed discussion in following the subsections.

I. The Scope of Legislative Interference

The scope of legislative intervention in any field depends mainly upon the nature of the problems arising from the subject in question. Legislative intervention may not achieve the desired result if not based on a well-grounded understanding of the social, economic and technical aspects of the subject in which the legislator intervenes.

As seen in Section B of this Article, crimes linked to computers are multitudinous and can be classified into several categories. The most acceptable classification distinguishes crimes according to the role that a computer might play in a particular crime. According to these criteria, computer crimes are divided into three categories; first, crimes where the computer is the 'object'; second, crimes where the computer is the 'subject' of a crime; and thirdly, crimes in which the computer is but an instrument for perpetrating traditional

[53] See, *supra,* note 9, 223.

[54] See, *supra,* note 4, 163.

[55] See, *supra,* note 26, 99-100; Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 JOURNAL OF HIGH TECHNOLOGY LAW (JHTL) 101 (2003), 102-3 ("Current criminal laws are unable to respond quickly to the rapid changes in Internet technology").

[56] See, *supra,* note 3, 795 ("Because of a lack of previous experience in dealing with computer crime and a dearth of reliable statistics upon which to base informed opinions, legislators, computer crime experts, and computer technologists find themselves differing sharply on the best legislative approach to the problem. They disagree on whether to enact completely new legislation or to amend existing laws, and whether support federal or state legislation, or both").

offences.[57] The question here is whether it is necessary for the legislator to criminalize all kinds of such crimes?

The majority of legal scholars confirm that new criminal provisions are needed to cover only those crimes that are unique to computers themselves. Other crimes in which the computer is used solely as the instrument of perpetration are either covered by existing criminal provisions or can be covered by simple amendments of such provisions.[58] According to one commentator writing on Michigan's computer crime laws: "[w]hile the Internet presents new problems for fighting crime, prosecutors should not be deterred from charging traditional crimes committed through the use of a computer using existing Michigan laws. Laws on communications offences, obscenity, solicitation of minors and child pornography, sales of controlled substances, fraud, and other crimes, are available to prosecute crimes committed over the Internet".[59]

In the light of these facts, the first and most crucial task for lawmakers is to determine and identify which crimes are truly unique to the computer. The precise determination of these crimes will be explored further in Section D of this Article, but at this point it is only necessary to point out some examples of computer crime statutes in jurisdictions where the legislators have not been successful in their intervention.

Looking at the United Arab Emirates (UAE) Law on The Prevention of Information Technology Crimes (2006), we discover that rather than applying the criteria developed by legal scholars, many acts that are not unique to the computer have been criminalized and subjected to existing criminal provisions stipulated in the Federal Penal Law. For example, Article 8 of the law criminalizes the act of eavesdropping communications transmitted across the Internet or through an information technology device[60], despite the fact that eavesdropping is not unique to computers nor its related devices and could feasibly be submitted to Article 380 of the Federal Penal Law No. 3 of 1987. Further, Article 9 of the law criminalizes blackmail and the issuance of threats through the Internet or an

[57] See, *supra,* notes 25-33, and accompanying text.

[58] See, e.g., *supra,* note 15, 500 ("The proper focus of computer-related crime statutes should be those crimes that are unique to computers themselves, not crimes that are facilitated or furthered through the use of a computer."); Stephen P. Heymann, *Legislating Computer Crime*, 34 HARVARD JOURNAL ON LEGISLATION (HARV. J. ON LEGIS.) 373 (1997), 380 ("For the most part, the federal criminal court already adequately covers crimes, such as the bank teller's embezzlement, in which a criminal uses a computer merely as a tool").

[59] Patrick Corbett, *Michigan's Arsenal For Fighting Cybercrime: An Overview of State Laws Relating to Computer Crimes*, 79 MICHIGAN BAR JOURNAL (MICH. B.J.) 656 (2000), 657.

[60] Article 8 of 'Law on The Prevention of Information Technology Crimes' stipulates that "anyone who intentionally and unlawfully eavesdrops, receives or intercepts communication transmitted across the Internet or an information technology device shall be liable to imprisonment, a fine or both".

information technology device[61] even though Articles 351 and 352 of UAE Penal Law are quite suitable for prosecuting such criminal acts. These examples indicate that the Law on The Prevention of Information Technology Crimes has created many cases of conflicting criminal provisions. The same is true of the *Law on Preventing Misuse of the Communication Equipments* No. 6 of 2006, promulgated in the Iraqi Kurdistan Region. In a comprehensive study conducted by the author of this Article, it has been found that almost all acts that have been criminalized by this law were already criminalized by the *Iraqi Penal Code* (1969) nearly forty years ago.[62] For example, the law criminalizes the act of intentionally disturbing others through the exploitation of a cellular phone, any kind of cable or wireless communications equipment, or the Internet or electronic mail, even though these acts have been criminalized by article 363 of *Iraqi Penal Code* since 1969.[63]

However, the legislator's mission does not come to an end simply by creating new criminal provisions criminalizing offences unique to the computer. Any intervention must also amend existing criminal laws. This is necessary for addressing two kinds of cases: firstly, those in which the computer makes the perpetration of traditional crimes easier, or more dangerous, compared to traditional perpetrations. Secondly, criminal laws should be amended where intangible properties related to the computer come under threat by criminal activities.

Regarding the first class of cases, the experience of the past three decades demonstrates that the computer has enhanced the ability of criminals in implementing criminal projects in many ways. For instance some traditional crimes, originally only possible through the co-operation of several individuals, are now, in the computer era, easily undertaken by a single person[64] who is capable of completing his criminal project from inside a home or work office possibly located thousands of miles away from the victim's location.[65] Experience also demonstrates that the utilization of the computer in the perpetration of some traditional crimes results in more dangerous consequences. For example, spreading

[61] This article provides that "anyone who uses the Internet or an information technology device to threaten or blackmail another to act or not act shall be liable to imprisonment for up to 2 years and a fine not exceeding AED 50,000 or either. If threat is used to induce the commission of a felony or cause defamation, the penalty shall be imprisonment for up to 10 years".

[62] See, Rizgar M. Kadir, *Remarks on the Law on Preventing Misuse of the Communication Equipments No. 6 of 2006*, 35 TARAZU ACADEMIC JOURNAL, 105 (2008).

[63] Article 363 of *Iraqi Penal Code* (1969) provides that "Any person who intentionally disturbs other by the abuse of cable or wireless communications equipment is punishable by a period of imprisonment not exceeding 1 year plus a fine not exceeding 100 dinars or by one of those penalties".

[64] See, *supra,* note 17, 1006.

[65] See, *supra,* note 5, 48.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

one computer virus might hit millions of computers around the world and cause billions of dollars in damages.[66] As such, legislators must intervene and consider the use of the computer in such crimes as an aggravating circumstance and increase the penalties attached.[67]

The notion of increasing punishment in some kinds of situations, known in the field of criminal law as aggravating circumstances, is not a new one and has been adopted by the penal codes in most countries around the world. One example of this is provided by the offence of theft in the *German Criminal Code*; the punishment prescribed for simple theft is a term of imprisonment not exceeding five years with the possibility of substituting it for a fine[68], while the punishment for a theft in which the perpetrator uses counterfeit keys might be a term of imprisonment not exceeding ten years.[69] In the same context, German legislators have laid down more severe punishment for robbery when the offender carries an instrument, weapon or means for overcoming the resistance of another person by force or the threat of force.[70]

There are also examples in which the legislator has increased the punishment where the criminal act results in more dangerous consequences. The offence of 'sexual assault by use of force or threats' in the *German Criminal Code* is just one such example; it is punished by a term of imprisonment not less than one year[71], but the penalty shall be imprisonment for life or not less than ten years if the offender, through sexual assault or rape, causes the death of the victim by gross negligence at minimum.[72]

As for the second class of cases, it is apparent that the computer has ushered in a new type of private property taking the form of intangible objects or electronic impulses such as computer data and programs. Given that the provisions of traditional substantive criminal

---

[66] See Eric J. Sinrod & William P. Reilly, *Cyber-Crime: A Practical approach to the Application of Federal Computer Crimes Law*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177 (2000), 218.

[67] See also, *supra,* note 21, 974 ("[T]he legislature might consider tying sentences to the gravity of the offense, using the value of data lost, stolen, or damaged as one factor, rather than as the sole factor in determining punishment"); Katyal, *supra,* note 17, 1076 ("Penalties would need to be revised as well, insofar as they were designed for an age in which crimes were tougher to solve").

[68] See, *supra*, note 51, Section 242(1).

[69] *Id.*, Section 243(1).

[70] See *Id.*, Sections 249(1) and 250(1)(b).

[71] *Id.*, Section 177(1).

[72] *Id.*, Section 178.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

law were drafted long before the invention of computers, the language of such provisions was too narrow to encompass violations directed at the new types of property that emerged with the computer.[73] When computer crimes statutes had yet to be enacted, prosecutors in many countries, when dealing with the destruction, sabotaging or copying of a computer program, faced real difficulties in submitting violations to existing traditional criminal provisions related to theft, extortion or larceny.[74] The earlier prosecutions of computer crime demonstrate just how far prosecutors tried to stretch the law to meet new circumstances. In the United Kingdom where *Computer Misuse Act* 1990 was not yet in force, the accused gained unauthorized access to a computer network and altered data contained on disks in the system. He was charged with damaging property under the *Criminal Damage Act* 1971. The prosecution faced a formidable challenge, as the *Criminal Damage Act* required proof of damage to *tangible* property. The prosecution claimed that the disks and its 'magnetic particles' contents were one entity, and by altering the state of the magnetic particles, the perpetrator damaged the disks themselves. The accused was convicted at trial, and appealed. The appeals court affirmed the conviction, holding that it was sufficient to prove that tangible property had been damaged, not that the damage itself was tangible. Damage was defined broadly to embrace the 'temporary impairment of value or usefulness'.[75] Similarly, in the United States "some courts have broadened the statute's reach by including computer data as a 'thing of value,' thus bringing the common crime of data theft within the [federal theft] statute's scope".[76]

In light of all these facts, the second area of law that must be amended by legislators is that related to the intangible and unique nature of computerized properties.

II. The Nature of Computer Crime Statutes

We will now turn our attention to the nature of computer crime statutes and the methods that legislators might adopt in providing the legal system of their countries with new substantive criminal provisions enacted specifically for combating computer crimes.

The experience of countries where computer criminal provisions have been enacted indicates that the legislator possesses two options in dealing with the subject in question.

[73] See, *supra,* note 4, 163.

[74] See *Id.*, 163 ("An overview of the case law dealing with crimes involving computers indicates that the courts have had difficulty identifying and defining the "res" element in these cases").

[75] See, *supra,* note 5, 41.

[76] John Montgomery, *Computer Crime, White-Collar Crime: Fourth Survey of Law*, 24 AM. CRIM. L. REV. 429 (1987), 430-31.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

First, legislators might include the aforementioned criminal provisions in one separate code as one specific computer crime statute. Some leading industrialized countries in the world, such as the United Kingdom and United States, have pursued this strategy by adopting *Computer Misuse Act* in 1990 and *Counterfeit Access Device and Computer Fraud and Abuse Act* of 1984 respectively. A similar method has also been adopted by other countries in the world including Malaysia, which enacted *Computer Crimes Act* in 1997, and The United Arab Emirates, which enacted *The Federal Law on The Prevention of Information Technology Crimes in 2006.*

The second option is inserting the substantive criminal provisions related to computer crimes into the existing penal law of the country. This strategy has been adopted by many countries in the world such as Germany[77], Denmark[78], France[79], Switzerland[80] and Canada.[81]

Each method has its own advantages and disadvantages: inserting the new criminal provisions into the existing penal law preserves the unity of substantive criminal law of the country in one code and prevents the dispersion of criminal provisions into many separate laws. This method is also more useful for courts, prosecutors, legal scholars and even ordinary people as they keep the substantive criminal provisions related to computer crimes easily accessible. On the other hand, the inclusion of the aforementioned criminal provisions in one separate code as a specific computer crime statute provides at least one important benefit, in that it would create public awareness of computer crime, a factor often recognized as one of the key means for deterring computer crime.

[77] See StGB, Sections 202a, 202b and 202c. Section 202c has been implemented by the 41st amendment to StGB and came into effect on 11 August 2007. The 41st amendment also amended Sections 202a, 202b, 303a and 303b of StGB, which in substance criminalize illegal access to, and interception and interference of data and sabotage of computer systems and so make up the core computer crimes. Dennis Jlussi, Handle with Care – But Don't Panic, Criminalisation of Hacker Tools in German Criminal Law and Its Effect on IT Security Professionals, has been implemented by the 41st amendment to StGB and is in effect as of August 11, 2007. The 41st amendment also amended Sections 202a, 202b, 303a and 303b of StGB, which in substance criminalize illegal access to, and interception and interference of data and sabotage of computer systems. Dennis Jlussi, *Handle With Care – But Don't Panic, Criminalisation of Hacker Tools In German Criminal Law and Its Effect on IT Security Professionals*, EICAR-Newsletter, (May 2008), 3, available at: http://www.eicar.org/press/infomaterial/Eicarnews_Mai_2008_fnl.pdf (last accessed 14 June 2010).

[78] See, *Danish Penal Code*, Section 263.

[79] See, *French Penal Code* (1994), articles 323-1 to 323-3. These articles have been inserted to the code during the period of 2000-2004.

[80] See, *Swiss Penal Code*, article 143bis.

[81] See, *Criminal Code of Canada*, article 342.1.

D. Substantive Computer Offences

This section will be devoted primarily to the determination and identification of those crimes that are unique to the computer. This step is necessary for legislators because it will pave the way for successfully enacting specific computer crime legislation in the field of substantive criminal law.

The experience of both countries that have enacted specific computer crime legislation and international conventions related to computer crimes indicates four basic substantive computer offences: unauthorized access, unauthorized access with intention to commit a further offence, intentional unauthorized modification offence, and misuse of devices. To this effect, the United Nations Information Economy Report states that "[t]he computer integrity activities addressed in the international instruments can be broadly classified into four categories: offences concerning access to data and systems; offences relating to interference with data and systems; offences concerning the interception of data in the course of their transmission; offences concerning the use of tools or "devices" to carry out any of the above acts."[82]

The discussion of the above mentioned offences and determining their precise elements are beyond the scope of this Article. However, we will examine a general description of each of them below.

I. The Unauthorized Access Offence

The most common illegal conduct and the one most unique to the computer is unauthorized access. It "occurs whenever an actor achieves entry into a target's files or programs without permission. The actor may be a person or another computer, and the access may be achieved electronically (through passwords and other mechanisms) or physically (by, for example, breaking into a file cabinet and stealing a personal identification number ("PIN"))."[83] As the UN Manual has stated, the entry or the access "is often accomplished from a remote location along a telecommunication network, by one of several means. The perpetrator may be able to take advantage of lax security measures to gain access or may find loopholes in existing security measures or system procedures."[84]

[82] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD), INFORMATION ECONOMY REPORT, 235 (2005), available at: http://www.unctad.org/en/docs/sdteedc20051_en.pdf (last accessed 12 June 2010).

[83] See, *supra,* note 17, 1021.

[84] See, *supra,* note 7, 75.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

In some countries where specific legislation on computer crimes has been enacted, the 'mere' unauthorized access to a computer has been regarded as a crime in and of itself regardless of the motive the intruder may have or the amount of damage to the computer or its contents. Accordingly, a person who knowingly and intentionally, and without lawful authority, accesses any computer, computer system, computer network, computer software, computer program, or data contained in such a computer, computer system, computer program, or computer network shall be subjected to criminal liability. For example, Section One of the United Kingdom's legislation deems a person knowingly causing a computer to function with the intent of gaining unauthorized access to programs or data on the computer as criminal behaviour, regardless of whether the intent was directed at any specific data or program contained on any particular computer.[85] The United States *Computer Fraud and Abuse Act* of 1986[86] similarly makes it a felony to knowingly access a computer without authorization and with intent or reason to believe that the information obtained would be used to injure the United States or to benefit a foreign country.[87] Malaysia's *Computer Crimes Act* (1997) criminalizes any intentional access to a computer without authorization regardless of whether the security measures, such as password protections, are infringed in order to gain access to the computer. One commentator regards this as "a bold and decisive statement of Malaysia's intolerance of hacking and will undoubtedly reassure potential investors."[88]

In other countries, the mere unauthorized access in and of itself is not considered a crime; the German Criminal Code punishes unauthorized access only in cases where the accessed data are protected by security measures[89]. Similarly, in some jurisdictions the perpetrator has to have harmful intentions, as is the case in France[90] and Canada.[91]

---

[85] See, *supra,* note 14.

[86] Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (1988))

[87] See, Subsection 1030(a)(1) of Computer Fraud and Abuse Act of 1986, 18 U.S.C.

[88] Donna L. Beatty, *Malaysia's "Computer Crimes Act 1997" Gets Tough on Cybercrime But Fails to Advance the Development of Cyberlaws*, 7 PACIFIC RIM LAW & POLICY JOURNAL (PAC. RIM L. & POL'Y J.) 351 (1998), 359.

[89] See, *supra*, note 51, Section 202a(1) which reads in full: "[w]hosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment of not more than three years or a fine". The English version is from Prof. Dr. Michael Bohlander's translation of StGB. Full text of this version is available at: http://www.gesetze-im-internet.de/englisch_stgb/index.html (last accessed 12 June 2010).

[90] See, *French Penal Code*, article 323(1).

[91] See, *Criminal Code of Canada*, article 342.1(1).

On the international level, Article 2 of the EC Convention on Cybercrime[92], labels this offence as 'illegal access', and obligates its parties to criminalize access to the whole or any part of a computer system without right, leaving it to the national legislatures to require, as an element of the crime, that the crime be committed by infringing security measures with the intent of obtaining computer data or other dishonest intent either directly or through a computer system connected to another computer system.[93]

Unauthorized access should be recognized as a stand-alone criminal offence for many strong justifiable reasons. On this point, the Explanatory Report to the Convention on Cybercrime states that "[i]t may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery".[94]

II. Unauthorized Access with Intention to Commit a Further Offence

This offence is more serious than the former[95]. Accordingly, it deserves more severe punishment. This offence occurs whenever an actor facilitates the commission of certain offences or commits unauthorized access in order to commit certain offences. Since this offence is more serious, the penalty upon conviction in British legislation is up to five years in prison, a fine, or both.[96]

---

[92] Council of Europe Convention on Cybercrime, 23 November 2001, C.E.T.S. No. 185, concluded and opened for signature, entered into force Jul. 1, 2004, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last accessed 14 June 2010).

[93] Article 2 reads in full: "[e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system".

[94] Explanatory Report to the Convention on Cybercrime, no. 44, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last accessed 14 June 2010).

[95] See, *supra,* note 15, 498.

[96] See, *supra* note 17, section 2(5)(b). The penalty for the Unauthorized Access Offense is a fine, up to six months prison, a fine, or both. *Id*., section 1(3).

III. The Intentional Unauthorized Modification Offence

This crime occurs whenever an actor does any act that he or she knows will cause the unauthorized modification of a program or data. This conduct is labeled 'data interference' and regarded as another stand-alone offence by Article 4 of Convention on Cybercrime. Paragraph 1 of the Article provides that "[e]ach Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right".

The aim of criminalizing this conduct is "to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage"[97], and the legal interest to be protected is "the integrity and the proper functioning or use of stored computer data or computer programs".[98] Paragraph 2 of the same Article allows States party to the Convention to enter a reservation concerning the offence and the option for requiring that the conduct result in serious harm.[99]

According to the *Computer Misuse Act* (1990), it is a crime to undertake any act that will knowingly cause the modification of a program, even if the actor does not target a specific computer, set of data, or program.[100] However, the actor's intent need not be directed at any particular computer, program, or data, nor concerned with any particular modification thereof.[101]

IV. Misuse of Devices

Despite the fact that the three offences discussed above are the basic substantive offences and, taken in combination, cover the vast majority of crimes specific to computers and computer technology[102], it is nevertheless a prudent preventative measure to criminalize

[97] See, *supra,* note 94, no. 60.

[98] *Id.*

[99] Paragraph 2 provides that "a Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm".

[100] See, *supra,* note 14, Section 3.

[101] *Id.*, Section 3(3).

[102] See, *supra,* note 15, 499.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

misuses of devices usually used in the perpetration of most computer crimes. These criminalizations are intended to address those who supply or possess tools used to intercept communications or access or interfere with data or systems.[103] The Explanatory Report has aptly described the purpose of such criminalization in stating that "the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5".[104]

Such criminalization might include the production, sale, procurement for use, import, distribution and making available of any of such devices including computer programs designed or adapted primarily for the purpose of committing any computer crime.[105]

The wording of criminal provisions related to the misuse of devices mentioned above presents a real challenge to lawmakers as they face the traditional problem of dual-use, which occurs frequently in criminal law. Dual-use occurs when broad categories of action are neither inherently bad nor inherently good, or whenever a technology can be used both for legitimate ends and for criminal purposes. The difficulty in dealing with such actions and technologies legislatively lies in the need of encouraging technological innovation while simultaneously discouraging its misapplication.[106]

The drafters of the Convention on Cybercrime faced the same problem when wording Article Six of the convention devoted to criminalization of misuse devices. They debated at length and considered four alternatives in dealing with the problem; first, restricting the devices to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This alternative, however, was considered to be too narrow: it could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The second alternative was the inclusion of all devices even if they are legally produced and distributed, but this was also rejected. The third alternative was the reliance on the subjective element of the intent of committing a computer offence, but this was also rejected given that it had not been adopted in other areas such as money counterfeiting.

[103] See, *supra,* note 82, 236.

[104] See, *supra,* note 94, no. 71.

[105] See, e.g., *supra*, note 51, Section 202c entitled 'Acts preparatory to data espionage and phishing'.

[106] See, *supra,* note 28, 266; *supra,* note 17, 1050.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press

The fourth alternative, which was lastly adopted as a reasonable compromise, was restricting the scope of the Convention to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. The drafters believed that this alone would serve best to exclude dual-use devices.[107]

E. Conclusion

Computer related misconduct began to appear shortly after the beginning of the widespread use of computer technology in Western societies. When computer crime statutes had yet to be enacted, computer crimes were subjected to traditional criminal laws, a policy that resulted in greater expense and other considerable difficulties. These problems and difficulties paved the way for the emergence of a consensus calling for legislators to intervene and enact specific computer crime legislation suited to confronting this new type of criminal activity. Many countries in the world responded by enacting new criminal legislation and many others are on their way to take similar legislative steps.

In order for the legislative intervention to be sound and successful there should be, on the part of those preparing and discussing legislative proposals and drafts, a solid understanding of the social, economic and technical aspects of the problems and misconducts attached to the computer and the Internet. Without this foundational understanding, the new criminal provisions might result in negative consequences.

Particularly, two major questions should be adequately addressed by legislators; the scope of legislative intervention and the nature of computer crime legislation enacted. Regarding the first question, new criminal provisions are needed only to cover those crimes that are unique to computers themselves. These include unauthorized access, unauthorized access with intention to commit a further offence, intentional unauthorized modification offences, and misuse of devices. Other crimes in which a computer is used simply as an instrument for perpetration are either covered by existing criminal provisions or can be covered by simple amendments of said provisions.

[107] See, *supra,* note 94, no. 73. Paragraph (1) of the article 6 of the Convention has been formulated as following "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: (i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches".

The second step that should be taken by legislators is the amendment of existing criminal laws with an aim to cover two kinds of cases: firstly, cases in which the computer is used as an instrument for committing known traditional crimes, making the perpetration of such crimes easier or resulting in more dangerous consequences compared to their more traditional forms. Secondly, cases in which intangible digitized property comes under threat from criminal activities.

While many countries in the world have soundly followed such a method in dealing with computer related misconducts legislatively, others have failed to do so. In some countries, the legislator has criminalized some criminal conducts that have long since been criminalized by that country's penal code. This creates conflict between criminal provisions, posing problems to prosecutors and courts alike.

Regarding the nature of computer crime statutes, the legislator is presented with two options. The first is the inclusion of the aforementioned criminal provisions in one separate code as one specific computer crime statute. The second is inserting substantive criminal provisions related to computer crimes into the existing penal law of the country. While the first method preserves the unity of substantive criminal law of the country in one code and prevents the dispersion of criminal provisions into many separate laws, the second one would, by contrast, create much-needed public awareness of computer crime.

https://doi.org/10.1017/S2071832200018757 Published online by Cambridge University Press