ПРАВО І БЕЗПЕКА 2003/2'1 ISSN 1727-1584

UDC 343.791:004

EDWARD CARTER[1]

Assistant Attorney General for the State of Illinois (USA) and Supervisor of Financial Crimes Prosecution for the Illinois Attorney General's Office

EXAMINING CYBERCRIME: ITS FORMS AND ITS PERPETRATORS[2]

The paper examines the nature and classification of cybercrime in the USA. Special attention is paid to legal aspects of cybercrime and cyber evidence. Procedural issues for obtaining of cyber evidence is given.

The term "cybercrime" is a broad term that is usually applied to a broad range of crimes in which computers are, in some manner, involved. This term, however, is vague and actually refers to a collection of dissimilar forms of criminal conduct that are powered by different motives. In this sense the term "cybercrime" is no different from the imprecise terms used to describe other forms of loosely related but analytically distinct criminal conduct. The term, "murder," for example, actually describes a number of different types of unlawful killing, e.g. first degree murder, second degree murder, and felony murder, all of which are powered by disparate motives, e.g. rage, greed, in some instances thrill, and money. Just as it is helpful to distinguish between the different forms of that collection of criminal conduct we broadly but imprecisely call murder, it is equally helpful to distinguish between the different forms of criminal conduct we broadly and imprecisely call cybercrime.

Every computer system is threatened by the large number of crimes we call cybercrimes, but every computer system does not face an equal risk of being victimized by all of those crimes. An engineering firm that designs parts for diesel locomotives, for example, faces a low risk of attacks from hacktavists and cyberterrorists and a high risk of having its computer system targeted for industrial espionage Understanding the distinctions between the various types of cybercrimes and the differing motives of cybercrimes perpetrators permits an intelligent evaluation of the threats they pose to different cybersystems. This type of threat analysis also facilitates an intelligent and efficient allocation of anti-cybercrime resources to the specific threats faced by a cybersystem, permits law enforcement to better focus its resources when investigating a particular cybercrime, and can assist lawmakers in designing more effective statutes to fight cybercrime.

This article is divided into two parts. Part one examines the nature of cybercrime, i.e. the different groups of offenses that are usually referred to as cybercrimes, and part two examines the types of persons who perpetrate cyberoffenses and briefly discusses the types of statutes used to prosecute them[3].

1. The Nature of Cybercrimes

Many people in law enforcement identify three distinct groups of cyberoffenses: A) offenses where the computer is the target of a crime, B) offenses where the computer is the tool used to commit the crime; and C) offenses where the computer is the repository of evidence of a crime This section of the article examines the differences between each of these groups. It should be noted, however, that these are not rigid categories and that as committed a particular cybercrime may actually be a hybrid of two or more of these offense types. Thus, for example, when a taxpayer's computer contains records reflecting his true sales and he uses his computer to electronically file a tax return that falsely understates gross sales, the computer is both the tool used to commit the crime of tax fraud and the

[1] Edward Carter is an Assistant Attorney General for the State of Illinois (USA) and Supervisor of Financial Crimes Prosecution for the Illinois Attorney General's Office. Prior to being named Supervisor of Financial Crimes Prosecution, Mr. Carter was a prosecutor in the Revenue Prosecutions Unit of the Illinois Attorney General's Office where he prosecuted various types of tax crimes, including the largest Motor Fuel Tax fraud prosecution in Illinois history, the largest Use Tax fraud prosecution in Illinois history, and, after Illinois became a party, the first prosecution in the United States under the International Fuel Tax Agreement. Mr. Carter is a graduate of Illinois Institute of Technology/Chicago-Kent College of Law. The views expressed in this article are those of the author and do not necessarily reflect the views of the Attorney General of Illinois

[2] This is the first in a series of two articles about the nature and prosecution of cybercrime. These articles are based on a lecture given by the author for the National University of Internal Affairs in Kiev, Ukraine, on October 15, 2002.

[3] Because of the federal system of government in the United States the vast majority of the cybercrime committed in the United States is investigated and prosecuted by the states and using state law Most of the statutes discussed here are Illinois statutes. Some American states have more experience than others in writing criminal statutes for cybercrime and in investigating and prosecuting cybercrime. As one of the larger industrial states and with Chicago and its large financial and commodities markets, Illinois is probably ahead of most American states in terms of cybercrime statutes and cybercrime investigation and prosecution.

ISSN 1727-1584

repository of evidence of that crime.

A. Computer as Target of Crime

One commonly identified category of cybercrime consists of those forms of criminal conduct in which the victim's computer is the actual target of the perpetrator's actions. In this type of offense the perpetrator's purpose is not to steal data or software, but is, instead, to alter the data or the software contained in the victim's computer. A common example of a computer as target offense is where the perpetrator accesses the victim's computer for the purpose of planting a destructive virus.

Other examples of computer as target offenses are denial of service attacks, such as when the perpetrator directs hundreds of messages to a victim's computer system so that the victim's customers are unable to access it, and business operations attacks, such as where a perpetrator accesses a pipeline company's computer and alters the program that controls the delivery and destination of oil or where a perpetrator accesses a power company's computer for the purpose of disrupting the delivery of electric power.

Computer as target crimes are usually not engaged in for the purpose of financial gain. In most instances they are engaged in for the purpose of disrupting business or governmental operations[4]. This disruption can be expensive. One leading American manufacturer that is a frequent target of cyberattacks calculates that it costs the company more than $157,000 per hour for each hour that its system is down.

B. Computer as Tool to Commit an Offense

A second commonly identified group of cybercrimes consists of traditional offenses that are committed by using a computer. Usually these traditional offenses include crimes such as embezzlement, forgery, theft, or gambling. A strong argument can be made that when these types of offenses are committed with the use of a computer they are not cybercrimes at all and should, in fact, be considered as nothing more than traditional crimes committed by a different means. Murder is classified as murder without regard to the means used to commit it, and there does not seem to be a strong reason to think of a traditional crime such as forgery as being different just because a computer is used to commit it. The cybercrimes in this group are the most frequently committed types of cybercrimes.

In some instances the crime committed with the computer may not, for technical or other reasons, fit within the statutory definition of a traditional offenses even though the result brought about by the use of the computer is clearly within the concept of a traditional criminal statute. Thus, whether forgery committed with a computer includes the making of a false electronic record may depend on how the term "document" is defined in the a forgery statute and whether using a computer to steal data or trade secrets constitutes theft will depend on whether the term "property" in a theft statute includes intangible property.

C. Computer as Repository of Evidence of a Crime

The third commonly identified group of cybercrimes crimes consists of offenses in which a computer is simply a repository of evidence of some type of offense. An example of this category of cybercrime is the drug dealer who, like any legitimate businessman, keeps his financial records and customer lists in a personal computer. Analytically, it seems incorrect to classify almost any of these types of offenses as cybercrimes because, with the exception of those cases such as child pornography where mere possession of the electronically stored image is a crime, a computer is not involved in their commission.

Most of the repository type offenses are what might be called criminal enterprise offenses in which the perpetrator is engaged in some type of illegal business such as drug dealing, prostitution, or illegal arms sales and keeps his records electronically[5]. This category of offenses also includes legal income offenses such as tax evasion where the perpetrator is engaged in a legal business but evades taxes and keeps his true business records in an electronic format. Finally, this category of offenses also includes contraband offenses where the computer contains materials, such as child pornography, in an electronic form that it is illegal to possess.

Repository offenses pose several challenges for law enforcement, the most important of which is how to acquire the electronically stored evidence. Should investigators obtain a search warrant authorizing them to seize the contents of the computer or a search warrant that authorizes them to seize the computer itself? When the use of personal computers for the storage of business records first became widespread, law enforcement almost always sought to seize the computer. Seizure of a business's computers often created problems because it usually resulted in a shutdown or a major disruption of the targeted business. One result of this was that judges were sometimes reluctant to issue a computer search warrant or demanded more evidence of probable cause than they required for traditional search warrants.

To avoid those problems, in legal business investigations search warrants now are generally sought only for the data in the computer rather than for the computer itself. In these cases hard drives are mirror imaged at the search site. When, however, law enforcement is investigating a criminal enterprise where there is little concern about and usually even a desire to shut down the illegal business, law enforcement continues to seek search warrants for the computer itself.

[4]In some instances the disruption may result in pecuniary gain to the perpetrator. Such gain, if the perpetrator considers it at all, is almost always a secondary consideration.

[5]Those engaged in criminal enterprises, no less than those engaged in a legal enterprise, must keep accurate business records or, like the proprietors of legal enterprises, they will soon be out of business.

ISSN 1727-1584

A second problem faced in repository offenses is when the evidence is not stored in the computer for which the search warrant is sought, but is, instead, stored in some other offsite computer or server which the computer to be searched is configured to access. A search warrant issued for a specific computer or computers does not authorize the search of a server or other computer not described in the warrant nor does such a warrant, without more, authorize using that computer to search other offsite computers or servers. To address this so-called "server problem," when law enforcement seeks a search warrant for data in a particular computer, it includes within the petition for the search warrant a request that the search warrant be for that computer *and for any server which that computer is configured to access*. That language allows law enforcement to access offsite servers that may actually contain the evidence or contraband being sought.

When the server is located outside the jurisdiction of the sovereign issuing the search warrant there may, of course, be a question about whether the search of the extra-territorial server is legal under the laws of the sovereign in which the server is located. At least under American law an argument can be made that this is an irrelevant issue.

Historically, the common law was unconcerned with whether or not evidence of a crime was obtained illegally[6]. As long as evidence could be authenticated it was admissible without regard to how it was obtained[7]. The exclusionary rule[8] was formulated to bar the introduction of evidence obtained in violation of the United States Constitution[9] Evidence obtained pursuant to a properly issued search warrant, even if that evidence was obtained by accessing a server located within the boundaries of a different sovereign and in violation of the laws of that sovereign would not have been obtained in violation of American statutory or constitutional law and thus theoretically, should not be subject to the exclusionary rule.

Finally, in repository offenses the use of a computer forensics expert is critical to ensuring that the evidence downloaded or printed out from the computer will be admissible. When executing the cyber search warrant law enforcement officers should be instructed not to touch the computer or anything in the room in which the computer is located, including light switches, until the computer forensics expert has secured the computer itself[10]. Once the area to be searched has been secured the computer forensics expert should be the next law enforcement officer to enter the area where the computer is located

2. Cybercrime Threat Sources

Cybersystems are subject to criminal threats from numerous type of cybercriminals. Generally cybercriminals can be grouped into three broad threat categories. These threat categories are distinguished primarily by the motive that powers the conduct of the perpetrators. The three threat sources are: A) hacker threats; B) traditional criminal threats; and C) ideological threats. This section of the article looks at the perpetrators of the crimes in each of these threat categories and examines the prosecutorial and judicial responses to them. It should be noted that the threat categories discussed below are neither rigid nor completely discrete and that sometimes there is overlap and crossover between them. Thus, for example, a hacker can move into the traditional criminal threat category if he begins to hack for pecuniary gain.

A. Hacker Threat

Hackers are persons who are motivated by the intellectual challenge of breaking into a computer system and by what some hackers describe as the "cerebral rush" that comes with a successful break in. Hackers are distinguished from traditional criminals by the fact that they do not engage in their conduct for direct pecuniary gain and are different from cyber-ideologs because they are not acting for ideological or political reasons. None of this is meant to suggest that the hackers are benign cybernerds. Frequently hackers are destructive and take pleasure in demonstrating their power by disrupting a computer system or network.

Some hackers and some observers of the cyberworld like to distinguish between so called "white hat" hackers and "black hat" hackers[11]. White hat hackers see themselves as "good guys" because after they break into a computer system they notify their victim of its security flaws.

Within the white hat category there are really two subcategories of hackers. One category is the so-called permissive hacker. Permissive hackers break into a computer system with the consent of the system owner and then advise the owner about the security defects they find.

[6]*United States v. Blue*, 384 U.S. 251 (1966); *Olmstead v. New York*, 277 U.S. 438 (1928).

[7]*Id.*

[8]The exclusionary rule is a judicially crafted rule that requires suppression of illegally obtained evidence. In the case of unconstitutionally obtained evidence the rule requires that the evidence as well as any evidence obtained from leads developed from that evidence be suppressed. This is called the "fruit of the poisonous tree" doctrine.

[9]*Rakas v. Illinois*, 439 U.S. 128 (1978).

[10]Some sophisticated criminal enterprises have programmed computers to destroy data at the touch of any key on a keyboard or the flick of a light switch in a room that is not preceded by entry of a password or code. More recently, terrorists have added explosives to the mix so that the flick of a light switch before entry of a password or code into a computer will set off an explosion that destroys the computer and kills those in the room or building.

[11]These labels are drawn from stereotypes found in old American western movies in which the hero or "good guy" almost always wore a white cowboy hat and the antagonist or "bad guy" almost always wore a black cowboy hat.

ISSN 1727-1584

Categorizing this type of hacker as a hacker at all seems to be analytically incorrect. A person who is retained to break into a building to test an alarm system is not called a white hat burglar. Indeed, he is not called a burglar at all He may be a security consultant, but the consensual nature of the break-in takes him out of the burglar category. To suggest that it should be otherwise in the cyberworld would seem to be intellectually lazy and blur the important distinction between a legal cyber-entry and an illegal one.

The other category of white hat hacker is the non-permissive hacker This type of hacker breaks into a computer system without the consent of the owner and then notifies the owner of the security flaws he finds. The non-permissive hackers' motives are, however, not completely altruistic because most are hoping they will be offered a reward or a job for their work. In the real world such a person at a minimum be considered a trespasser who has committed a tort for which he may be sued civilly and a crime for which he may be criminally prosecuted[12]. Also in the real world, such conduct would most probably be viewed by many as nothing more than a subtle form of extortion. Why it should be seen as anything different in the cyberworld is unclear. Thus, non-permissive white hat hackers might more appropriately be classified as gray hat hackers or worse because they are engaging in illegal conduct and are doing so for other than completely altruistic reasons.

The other category of hacker, the so-called black hat hacker, breaks into computer systems for the thrill or doing so and does damage to or alters software, data, or systems.

Hackers, who are usually 15 to 24 years old, are virtually always an external threat source and are usually male. Indeed, one study done by professor Nicholas Chandler of Queensland University of Technology in Brisbane, Australia suggests that 95 % of all hackers are male. Many hackers erroneously believe that if they are caught before they reach age 18 they will be prosecuted under the much more lenient juvenile justice statutes. As result quite a few hackers quit hacking when they reach 18[13].

There are a number of informal and formal responses that can be made to the hacker threat. The most important and probably the only informal response to the hacker threat is for systems owners to greatly increase the sophistication and strength of their cyber-security systems.

The criminal justice system, however, has a host of formal responses to the hacker threat. In Illinois, one of those responses was the adoption of a statute that creates a crime called Computer Tampering.[14] This statute criminalizes accessing a computer without authority and contains sanctions of graduating severity (from misdemeanors[15] to low level felonies[16]) depending upon whether the conduct involves access only, access and obtaining data or programs, access and damaging data or programs, or access and insertion of data or a program. Illinois has also created an offense called Aggravated Computer Tampering[17] This offense makes it a Class 2 felony to access a computer and disrupt vital government service, public utility service, or create a strong probability of death or great bodily harm.

Besides the specifically defined computer offenses, other criminal charges that are frequently brought, depending on the hacker's conduct, are forgery for creating false electronic records, i.e. records that are initially created electronically and stored electronically and which are altered while in electronic form[18].

---

[12]Some commentators argue that the real world concept of trespass does not work in the cyberworld. Even if one rejects the application of the trespass concept in the cyberworld, the idea that unauthorized entry into parts of a cyber system that are closed to the hacker and others should give rise to civil and criminal liability does not seem to be an unreasonable or unwarranted extension of the civil and criminal law.

[13]The hacker's belief about juvenile prosecution is incorrect. Under the law of many American states persons under the age of 18 may be prosecuted as adults. In Illinois 17 year olds who commit crimes are subject to prosecution as adults. In one Illinois cybercrime investigation the 17 year old perpetrator defiantly told the investigator that he was 17 and nothing was going to happen to him. That perpetrator was unpleasantly surprised when he was charged as an adult and learned that he was old enough to be sent to prison.

[14]*Ill. Comp. Stat.*, Ch. 720, §5/16D-3.

[15]A misdemeanor in Illinois is an offense for which the potential sentence is imprisonment for less than one year *Ill. Comp. Stat.*, Ch. 720, §5/2-11.

[16]A felony in Illinois is any offense for which the potential sentence is death or imprisonment for one or more years. *Ill. Comp. Stat.*, Ch. 720, §5/2-7. In Illinois felonies are classified as Class 4, Class 3, Class 2, Class 1, and Class X with Class 4 felonies being the least serious (Class 4 felonies carry a potential prison sentence of one to three years imprisonment) and Class X felonies being the most serious (Class X felonies carry a mandatory minimum sentence of six years imprisonment, meaning that when a defendant is convicted of a Class X offense the judge must sentence the defendant to at least six years in prison. The maximum Class X sentence is 30 years imprisonment. See, *Ill. Comp. Stat.*, Ch. 725, §5/5-8-1(a)(3). There are no Class X cybercrimes. Certain violent Class X felonies, such as First Degree Murder also carry a possibility of a sentence of death or life imprisonment.

[17]*Ill. Comp. Stat.*, Ch. 720, §5/16D-4.

[18]The crime of Forgery is an excellent example of updating an old crime to meet a new form of criminal conduct. Forgery in Illinois historically included the making of counterfeit documents. *People v Mau*, 377 Ill. 199 (1941); *People v. East-West University*, 265 Ill. App.3d 557 (1st Dist. 1994). In the late 1990's the Illinois legislature expanded the definition of the term "document" as that term is used in the Forgery statute so that it includes electronic records as that term is defined in the Illinois *Electronic Commerce Security Act*. See, *Ill. Comp. Stat.* Chap. 720, §5/17-3(c).

ISSN 1727-1584

Except in the cases of repeat offenders or cases of serious tampering, jail and prison sentences are seldom meted out to hackers. In most instances hackers receive sentences of probation for a period of 30 months with special conditions. The special conditions of probation usually require the defendant to pay restitution to the victim for damage caused by his conduct, perform a specific number of hours of Sheriff's Work Program[19], forfeit the computer equipment and software used to commit the crime, and, in some instances, require cooperation of the defendant in the prosecution of others involved in that or other crimes. In some instances, another special condition of probation is that the defendant not own a computer that is connected to the telecommunications system.

When cooperation is part of the sentence cooperation is usually defined to mean that the defendant will fully and truthfully answer all questions that are posed to him by investigators and that upon the request of the prosecutor, and without subpoena, the defendant will appear and give full and truthful testimony before a grand jury, at any court hearing or trial, and at any administrative proceeding.

B. Traditional Criminal Threat

A second threat category is the traditional criminal threat. This threat is posed by those who engage in cybercrime for pecuniary gain. Thus, while hackers, cyberterrorists, cyber-anarchists, and traditional cybercriminals are all engaging in criminal conduct, the traditionally motivated cybercriminal is different from other cybercriminals because the traditionally motivated cybercriminal commits the offense for monetary gain while the others are motivated by non-pecuniary or ideological reasons.

Unlike with the other types of cybercrimals, the traditionally motivated cybercriminal threat is almost always an internal one. A recent study of traditionally motivated cybercrime indicates that more than 80 % of the perpetrators are insiders. For law enforcement this presents both a problem and a benefit: it's a problem because initially law enforcement does not know if one or more of the victim's employees who they are interviewing is the perpetrator and it's a benefit because it means there is a small universe of people who are the most likely perpetrators.

Generally, decidedly "no-tech" methods are used to compromise cybersecurity The threat source in this class of crimes is usually either the disgruntled employee who steals or passes on information for monetary gain or the duped or blackmailed employee who is tricked or coerced into breaching cybersecurity. In one instance a perpetrator feigned romantic interest in a female employee of an insurance company and involved her in a scheme which resulted in a loss to the insurance company of more than $700,000.

Traditionally motivated cybercriminals usually engage in several distinct types of criminal offenses. One group of offenses frequently committed by traditionally motivated cybercriminals is intellectual property crime. One common form of intellectual property crime committed by computer is where a computer is used to steal trade secrets[20]. This form of cybercrime is really nothing more than what historically has been called industrial espionage Nation states also engage in this form of cybercrime to assist their domestic industry in product or technology development. According to a 1987 report from the U.S. Central Intelligence Agency, one priority of Japanese foreign intelligence in the early 1980's was to obtain information about technological and scientific developments in the United States and Western Europe.

Other forms of intellectual property offenses committed by traditional cybercriminals involve copyright and trademark violations. In copyright violations computers are used to copy and distribute copyrighted materials. While this form of crime usually is committed in the context of music and video recordings, it can also include the pirating of written materials. In trademark violations computers are used to counterfeit trademarks that are then affixed to cheaper, inferior quality goods. Because of the large sums of money businesses spend to build up good will for their trademarks and the reputation for quality which those marks are designed to represent, losses from this form of cybercrime can be large but difficult to calculate.

The problem of counterfeit trademarks is merely an economic one when associated with clothing and other trademarked items on whose performance human life does not depend. Trademark counterfeiting can, however, be life threatening when the counterfeit mark is affixed to inferior quality goods whose performance is not within engineering tolerances required to ensure human safety. Thus, trademark counterfeiting involving pharmaceuticals and aircraft, automotive, or machinery parts causes not only a financial loss to the trademark holder, but, poses a serious danger to the health and safety of the public at large.

Another form of cybercrime committed by traditionally motivated criminals is fund transfers. In fund transfer cases the perpetrator causes banks or investment firms to transfer funds or to sell securities and transfer the sale

[19]Sheriff's Work Program is a sentencing alternative to incarceration. The sentence is only available in those Illinois counties where the county sheriff has created such a program. Offenders sentenced to work in a Sheriff's Work Program perform different types of physical labor under the direct supervision of deputy sheriffs. The work performed is of a nature that benefits the entire community and is almost always done in public view. Usual forms of work include picking up garbage from streets or roadsides and clearing snow and ice from public sidewalks.

[20]As the term "trade secrets" is used here that term includes not only proprietary formulae such as the formula for Coca Cola, but also proprietary financial, engineering, and manufacturing data.

ISSN 1727-1584

proceeds from the victim's account to an account controlled by the perpetrator. While fund transfer schemes may employ a single large transfer, large transfers will usually raise red flags that will cause attention to be drawn to them.

A more frequently used alternative to the large fund transfer is the deminimis transfer. In deminimis transfer schemes the perpetrator causes the transfer of a very small amount from a large number of account holders. The amount usually will be less than a dollar or two, an amount that many account holders may not notice and which if they do many are likely to ignore. To the extent victims do complain, because of the small individual amount involved, the matter will most likely be handled by low level customer service employees who will not have sufficient information to see or the motivation to look for the larger pattern of criminal activity. The result is that this form of fund transfer scheme is discovered, if at all, long after the crime has been committed.

Counterfeiting schemes involving negotiable instruments have become a particularly ubiquitous form of cybercrime that has been made easy and inexpensive by the development of low cost scanners and simple but effective programs for altering scanned images. One of the most common of the counterfeiting schemes involves the counterfeiting and negotiation of checks. In these schemes the perpetrator buys check stock at an office supply store, use a computer to create checks drawn on the accounts of real businesses, and cashes them. By the time the check is identified as counterfeit[21] the perpetrator has moved on to a different locale and repeated the process.

Computers are also used in connection with the perpetration of various types of fraud schemes. These schemes include credit card skimming, telecommunications fraud, and fraudulent investment and loan schemes.

The crime of identity theft which has become rampant, is one of the few traditionally motivated cybercrimes that has no pre-cyber era cognate In most instances the individual's financial information is obtained in very simple and common ways. Among these are so-called "dumpster dives" in which the identity thieves go through garbage looking for a person's bank statements or credit card statements. Another way of obtaining a person's financial identity is for the perpetrators to pay for them. These payments are made to low level employees who, as part of their job, handle people's financial information. These employees can be hospital admitting clerks, car dealer employees, mortgage broker employees, and government clerks at tax and licensing agencies.

In one sophisticated scheme the perpetrators paid hospital admitting clerks for the financial identification of recently deceased patients. Using this information the perpetrators bought luxury cars with the maximum amount of financing. At the time of the purchase the perpetrators would buy credit life insurance. Thereafter they would make several payments and then advise the insurer that the insured had died. To substantiate the claim the perpetrators would obtain the purported buyer's death certificate, scan it into a computer and alter the date of death The insurance companies paid the claims, the decedent's heirs had no idea what had occurred, and the perpetrators would then resell the cars at large profits.

There are both formal and informal responses to traditionally motivated cyber threats. The most effective informal response to the theft of proprietary formulae is never to commit the formulae to an electronic form. Such formulae are best kept in typewritten form on photocopy proof paper. For large quantities of proprietary information, keeping data in a non-electronic form may not be practical. In these instances the business is best served by strictly limiting the number of employees who have access to the data, regularly reviewing the access list, closely supervising employees on the list, and removing any employees from the list who may have substance abuse, gambling, or other problems that may motivate them to engage in the criminal conduct.

There is no shortage of statutory tools to prosecute perpetrators of traditional offenses. Usually the much more difficult problem is identifying who the perpetrator actually is. In many U.S. states theft is one statute that can be used to prosecute traditional computer crime. In some U.S. jurisdictions theft is not a possible charge because the definition of property in their statutes includes only tangible property, i.e. property that is capable of being physically carried away, and does notinclude intangible property. Some U.S. jurisdictions have updated their statutes to include the theft of intangible property and others, such as the federal government, have simply enacted statutes aimed directly at the purloining of trade secrets.

In some U.S. jurisdictions, including Illinois, where the crime of Forgery includes the making of counterfeit documents the statute is used to prosecute cybercrimes involving computer assisted document counterfeiting. As discussed above, in Illinois the forgery statute has been modernized so that the term "document" in that statute is defined to include electronic records as defined in the Electronic Commerce Security Act [22] The practical conse-

[21]Identification may take several days because of the time necessary for checks to be processed after negotiation. This is a particular problem when the checks purport to be drawn on banks located in parts of the U.S. far from where the check is negotiated. The problem is exacerbated if the bank on which the check is drawn honors it. This frequently occurs when a small denomination check is scanned and is altered to a much larger amount. In these cases everything on the check except the amount is correct and it will easily pass through the banking system. In these cases it is not until the account holder complains that the counterfeiting is discovered

[22]*Ill. Comp. Stat.*, Ch. 720 § 5/17-3(b). The *Electronic Commerce Security Act, Ill. Comp. Stat.*, Ch. 5, §175/5-105, defines the term "electronic record" as a record generated,

ISSN 1727-1584

quence of that change is that the crime of Forgery now includes the creation of false electronic records even if those records are created electronically and not reduced to tangible written form until after the electronic record has been altered.

A large number of U.S. jurisdictions, including Illinois, have adopted a statute directed exclusively at crimes committed with computers. These computer crimes statutes generally make it an offense to use a computer in connection with a scheme to defraud[23] These statutes are usually quite broad and by their terms apply wherever a computer or program is accessed for the purpose of devising or executing a scheme to defraud or used to obtain money or property through such a scheme. Thus, under at least one prong, these statutes make it a crime merely to access a computer to advance a scheme to defraud, even if no one is actually defrauded and under a second prong they make it a crime to use a computer in a fraud scheme and thereby obtain money or property. The former category of offense is usually a low level felony, while for the later category, the seriousness of the offense ranges from a Class 4 to a Class 2 felony depending on the value of the property, money, or services obtained.

One of the most useful offenses for the prosecution of traditionally motivated cybercrime is the crime of Wire Fraud, an offense initially aimed at fraud schemes perpetrated by telegraph and telephone. In a brief, Wire Fraud makes it a crime to use the telecommunications or broadcast systems in connection with devising or perpetrating a scheme to defraud The Wire Fraud statute is valuable because it criminalizes the devising of a scheme and allows, without regard to the number of victims or whether anyone is actually defrauded, the prosecution of the entire scheme in one charge. Wire Fraud is also valuable because, at least under the Illinois statute, it specifically contemplates the prosecution of perpetrators who, from outside the state or even outside the United States, use telecommunications such as e-mail or the Internet to send communications into Illinois to perpetrate fraud schemes.

Traditionally motivated cybercriminals are much more likely to see prison sentences than hackers. Certainly, prosecutors will be much less likely to enter plea agreements that do not have a prison sentence, and, in non-agreed dispositions, will argue much more vigorously for prison sentence. Most sentences will also include restitution to the victims as an element of the sentence and forfeiture of the equipment used to commit the crime. Illinois sees forfeiture as an important element in the punishment and deterrence of computer crimes. This policy is reflected in the fact that Illinois' computer crimes statute has its own forfeiture provisions.

C. Ideological Threat Sources

Cybersystems face three ideological threat sources. a) anarchic threats; b) hacktavist threats; and c) terrorist threats. This section of the article examines each of these threat sources.

Anarchic threats are posed by perpetrators motivated by an ideology that information and access to information should be free. This is an ideology that is almost unique to the cyberworld. The cyberanarchist generally rejects all intellectual property laws and sees himself as a later day Robin Hood who takes data from rich information owners and makes it available to the poor, deserving public by posting the stolen data on various Internet sites. In fact, cyberanarchists are really nothing more than common thieves who do not understand that it is the very intellectual property laws they scorn that have made their computers and the Internet possible.

Cyberanarchists are generally prosecuted under computer tampering statutes or for Theft. At its most serious, computer tampering is the least serious felony under Illinois law. Because the seriousness of Theft is determined by the value of the data or information stolen, and high value means conviction of serious felonies, Theft is the better of the two charges to bring, assuming that the evidence supports that charge.

The second type of ideological threat is the hacktavist threat. Hacktavists are motivated by political ideology to attack specific sites as part of political protests. Thus, anti-free traders may try to hack into the World Bank's computer system as part of their protest against free trade and persons with human rights agendas may attack the computer networks of businesses that use low wage offshore suppliers. It would not be surprising to see hacktavists who oppose war against Iraq trying to attack computer networks of companies and universities that have contracts that support the war effort. This would be a logical progression from the real world protests at brick and mortar facilities by Vietnam War protestors who, together with younger anti-war activists now oppose either an Iraqi war or the war against the Al-Quaeda.

Hacktavist attacks generally take the form of intrusions that alter or destroy programs or data, denial of service attacks, and website defacement. The best available prosecutorial response to hacktavist attacks is to charge hacktavists with the offense of Computer Tampering or to charge them as a group with Conspiracy with Computer Tampering as the target offense.

The third type of ideological threat is from cyberterrorists. Cyberterrorists engage in conduct that constitutes cybercrime for the purpose of effecting political change through the intimidation of a substantial portion of the civilian population Because the purpose of the cyberter-

communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.

[23]Because these statutes are aimed at schemes to defraud they do not address crimes involving child pornography or the use of computers in perpetrating sex crimes against children. While that form of criminal conduct certainly can be classified as a cybercrime, that form of cybercrime is addressed by different statutes.

ISSN 1727-1584

rorist is to intimidate a substantial portion of the civilian population, the targets of cyberterrorists are likely to be the computer networks of public utilities such as water companies and telecommunications companies and the computer networks that control energy distribution system, such as the power grid and fuel pipelines.

If a cyberterrorist strikes a utility or government system and disrupts vital services or creates a substantial risk of death or great bodily harm, the perpetrator can be prosecuted for the offense of Aggravated Computer Tampering, a significantly more serious felony than ordinary computer tampering.

Received by Editorial Board on 28.03.2003

КАРТЕР ЕДВАРД. ДОСЛІДЖУЮЧИ КОМП'ЮТЕРНУ ЗЛОЧИННІСТЬ: ЇЇ ФОРМИ І ЇЇ ЗЛОЧИНЦІ (ЧАСТИНА ПЕРША)

Приведено аналіз поняття і класифікації комп'ютерних злочинів, які склалися в США на сьогоднішній день. Особлива увага приділяється питанням правової оцінки комп'ютерних злочинів і комп'ютерних доказів, описано процесуальний порядок отримання комп'ютерних доказів.

***

КАРТЕР ЭДВАРД. ИССЛЕДУЯ КОМПЬЮТЕРНУЮ ПРЕСТУПНОСТЬ: ЕЕ ФОРМЫ И ЕЕ ПРЕСТУПНИКИ (ЧАСТЬ ПЕРВАЯ)

Приведен анализ понятия и классификации компьютерных преступлений, которые сложились в США на сегодняшний день. Особое внимание уделяется вопросам правовой оценки компьютерных преступлений и компьютерных доказательств, описан процессуальный порядок получения компьютерных доказательств.

УДК 343.148

О.Ф. КОБЗАР

Кіровоградська філія Національного університету внутрішніх справ

ОСНОВНІ ПОЛОЖЕННЯ ПІДГОТОВКИ ТА ПРИЗНАЧЕННЯ СУДОВИХ ЕКСПЕРТИЗ

Запропонована система рекомендацій щодо постановки запитань експертам, які ґрунтуються на узагальненні та аналізі практики розслідування злочинів і призначення по ним експертиз.

Однією з умов високої якості розслідування злочинів при зібранні та аналізі доказів є широке використання спеціальних науково-технічних знань із різних галузей. Найбільш поширеною та ефективною формою їх використання в кримінальному судочинстві є судова експертиза. Експертизою на досудовому слідстві називають слідчу дію, регламентовану кримінально-процесуальним законом, яка полягає у дослідженні за завданням слідчого, особою, що володіє певними знаннями – експертом, наданих в його розпорядження матеріалів кримінальної справи, предметів і документів з метою встановлення фактичних даних, що мають значення для правильного її розв'язання.

Визнавши за необхідне проведення експертизи, слідчий, керуючись статтями 130 і 196 КПК України, зобов'язаний скласти про це мотивовану постанову. Реквізити цієї постанови також закріплені в ч.2 ст.196 КПК України.

У практичній діяльності слідчих органів склалась така форма постанови про призначення експертизи при якій:

- у вступній частині зазначається час (день, місяць, рік) та місце її складання, хто склав постанову, по якій кримінальній справі;

- у описовій частині коротко викладається суть справи, конкретні обставини, що обумовлюють необхідність проведення експертизи, зазначаються норми закону, на підставі яких призначається експертиза;

- у резолютивній частині формулюються питання, встановлюється, в разі необхідності, строк, призначається експерт або визначається експертна установа, до якої направляються матеріали, наводиться перелік матеріалів, що подаються на експертизу.

Особливий інтерес у даній постанові викликає складання резолютивної частини:

Перш за все, необхідно сформулювати питання. Вони не повинні виходити за межі компетенції та разом з тим повинні бути ретельно відредагованими, щоб уникнути некоректних питань (наприклад, чи не була потерпіла вагітною або чи не страждала вона іншою психічною хворобою?); крім того, питання повинні бути визначеними, чіткими, зрозумілими, та такими, що виключають їх неоднозначне тлумачення.