Abstract

White Collar crime is a dangerous problem that becomes even more dangerous when aligned with computer crime. These two types of crime feed on each other and present a global challenge to society and the police. The combination of these two types of crime can severely undermine the economy especially in developing countries. It is imperative, therefore, that the police be better trained in the sciences of forensic accountancy.

This paper presents definitions, classifications and profiles of how white collar crime and computer crime can be intertwined, who are involved, and the loopholes that allow financial assets to be moved undetected across the globe. The paper examines computer crimes as they practically progress at different stages. This examination addresses criminal techniques such as "trojan horses," "viruses," "salami," "logical bombs," and explain the risks that face society, in general, and public and private institutions, in particular, as a result of these criminal activities .

This paper also addresses the relationships between cyber crime, money laundering, and explains the practice of commingling licit and illicit assets. It makes a strong case for training the police in forensic accountancy, an emerging discipline by which police experts can collect direct evidence as well as circumstantial evidence and apply such scientific concepts as "sampling," "forecasting," "ratio analysis," and "flow charts."

This paper concludes by proposing an advanced protocol for police training. That protocol focuses on three distinct activities: (1) detection, (2) investigation, and "prevention." It also introduces the reader to available facilities and programs where the police can be trained to combat economic crimes.

The Challenges of White Collar Crimes and Computer Crimes and The Imperative of Training the Police in Forensic Accountancy

by
Sam S. Souryal, Ph. D.
Sam Houston State University
Huntsville, Texas

To be presented before the Sharjah Conference on Economic Crime,
January 21-22, 2002

Introduction

White collar crime has been a dangerous problem which is made more dangerous by the technology of computers. While the term only dates to 1939, white collar crimes have been practiced for centuries by kings and presidents, popes and generals, ministers of the church and ministers of government, as well as bureaucrats and corporate managers. They were then, as they are now, crimes of the "rich and the powerful." They are basically motivated by greed and carried out by means of deception, fraud, and extortion. In a sense, the concept of white collar crime has exposed the dualistic fallacy of the nineteenth century criminal type: (1) crime is committed only by the lower socio-economic class, and (2) law-abiding citizens are substantially different from those who fit the criminal type (Poveda, 1994:4). It was left to Sutherland in 1939 to resolve that fallacy by declaring that "white collar criminals are the upper world counterparts of professional thieves" (Geis et al., 1995:24). White collar crime continues in all nations, costing societies enormous losses economically, socially, and spiritually. In the United States, society continues to pay dearly for the suffering caused by Vietnam, Watergate, the Savings and Loan scandal, and, of course, addiction to drugs and cigarettes.

With the advent of computer technology, white collar crimes became easier, faster, neater, and much more difficult to detect. Especially in the banking industry, white collar criminals can now strike more aggressively against assets anywhere in the world. Through the use of sophisticated data communication systems, it is now possible, for example, to move huge accounts from one bank laundering them through several banks around the world, and re-deposit them as a legitimate new account, all with a few clicks on the computer's keyboard. The fed wire, one of three data communication networks connecting bank computers for the transfer of funds, is reported to "transmit an amount equivalent to the entire national debt every four days" (Parker, in Geis and Stotland, 1980:201). Financial statements

and confidential information, essential to white collar crime activities, are now readily available through service providers such as Internet, Microsoft Network, America On-line, Computer Service, and other data bases. Three of these companies, Computer Service, Prodigy, and America Online, have already secured more than 4 million subscribers, a number greater than the combined circulation of *USA Today* and *The Wall Street Journal* combined (Swanson, et al., 1996). As a result, white collar criminals can now carry out their illicit schemes with mathematical precision because of their access to secret accounts, financial assets, consumer listings, and corporate statements.

To make matters worse, financial assets, the principle targets of white collar crime are no longer contained in bank vaults or in written statements; they are recorded in data systems by electronic forms. As a result, it is estimated that through the combination of white collar crimes and computer technology, white collar criminals defraud the public of billions of dollars every year. On the positive side, however, it should be noted that unlike traditional white collar crimes that were growing steadily without being statutorily crimi nalized, the spread of computers has forced legislators to enact explicit and distinct criminal laws to deter illegal use.

In this article, I intend to present an examination of the socio-legal and economic views of white collar crimes as well as their characteristics, definitions, classifications, and cost to society. This will be followed by a detailed examination of computer crimes and money laundering as the principal requisites for white collar criminal activities. This article will conclude by recommending several policy implications pertaining to the investigation of these crimes and the training of investigators.

Sutherland's Theory of White Collar Crime

The term "white-collar crime" was coined by Edwin Sutherland when he addressed the American Sociological Association in Philadelphia in 1939. Sutherland forcefully brought the concept to the attention of the scholarly community and the world in his denunciation of what he called "the evil machinations at the expense of the public well-being" (Geis, Meier, and Salinger, 1995:2). Sutherland describes the environment of white collar criminality in these terms:

> *Present day white collar criminals, who are more suave and deceptive than the 'robber baroness' are represented by the princes and captains*

of finance and industry, and by a host of lesser followers. Their criminality has been demonstrated again and again in the investigations of land offices, railways, insurance, munitions, banking, public utilities, stock exchanges, the oil industry, real estate, reorganization committee, receiverships, bankruptcies, and politics. White collar criminality is found in every occupation as can be discovered readily in casual conversation with a representative of an occupation by asking him, what crooked practices are found in your occupation?" (Sutherland, 1940:30).

Sutherland describes white collar criminality in the fields of business by stating:

> *White collar criminality in business is expressed most frequently in the form of misrepresentation in financial statements of corporation, manipulation in the stock exchange, commercial bribery, bribery of public officials directly or indirectly in order to secure favorable contracts and legislation, misrepresentation in advertising and salesmanship, embezzlement and misapplication of funds, short weights and measures and misrepresentation of commodities, tax frauds misapplication of funds in receiverships and bankruptcies. These are what Al Capone called the legitimate rackets* (Sutherland, 1940:31).

Sutherland's reference to Al Capone and "the legitimate racket" is especially significant for a better understanding of white collar criminality. Al Capone was, of course, a notorious gangster in the 1930s who, despite all the violent crimes he committed, the FBI was only able to convict him on charges of tax evasion. Sutherland's reference to "the legitimate rackets," was, on the other hand, a clear reminder of the practice of gangsters and organized crime activities which was so skillfully camouflaged as to appear legitimate.

Sutherland's theory of white collar crime focuses, almost exclusively, on the violation of "trust, delegated or implied." Delegated trust are obligations assigned to a public official or a corporate manager by virtue of his official authority and, as such, are within his duty to preserve. Implied trust, on the other hand. constitutes obligations that are not explicitly authorized but are assumed by convention to be within the official's moral duty. Sutherland further asserts that violations of trust invariably fall within two categories: (1) misrepresentation of asset values, which in Sutherland's view, amounts to fraud or swindling, and (2) duplicity in the manipulation of power (Sutherland, 1945).

The former category needs no further elaboration, since (provided that all elements of the crime are proven) it presents society with a clear case of theft, thus making the public official as culpable as any other criminal. The second category is a little more tricky, since it assumes the practice of "double crossing." A good example would be the case of a corporation manager who, acting upon inside information, purchases land which the corporation will need in the future and then later he sells it at an exorbitant profit to the corporation. The basic principle in all such cases is "duplicity," an immoral behavior which is no less criminal in white collar crime than in common fraud crimes. Sutherland explains the concept of duplicity as "holding two antagonistic positions"; one is a position of trust that should always be upheld, and the other is in violation of trust in order to achieve "personal gain." Sutherland further adds that when public officials and corporate managers are compelled by law to make a separation of these two positions, "they make a nominal separation and continue by subterfuge to maintain both positions" (Sutherland, 1945).

Characteristics of White Collar Crimes

White collar crimes are offenses committed by persons of high social prestige in their occupations; hence, the label "white collar" as opposed to "blue-collar"-- the former characterizes the so-called "boardroom crimes," while the latter, "street crimes," and "occupational crimes" (see Albanese, 1995; Geis, Meier, Parker, 1983; and Saliner, 1995; Simon, 1996; Swanson, et al 1996;). These are "exotic crimes" the perpetrators in the past used to be called "robber barons," now it seems more fitting to be called "criminals in tuxedos."

White collar criminality is not a recent phenomenon. Aristotle, in *Politics*, was perhaps the first writer who called attention to white collar crimes committed by road commissioners in Athens, and the first law against white collar crimes is believed to be a 1473 English law prohibiting government agents from stealing goods or property placed in their care (Green, 1993:95). Given today's complex bureaucracies and business conglomerates, white collar crimes may be legitimately considered among the most sordid and inexcusable crimes in modern times. Like the offense of thievery in the Islamic tradition, white collar crimes "devour one's wealth by false or illegal means" (*Quran*, Chap.2 :188). But unlike thievery, White collar crimes are not direct attacks by a person on another's property; they brazenly and stealthily cause the demise of the entire society by laying its citizens' economic welfare prey to indiscriminate embezzlement (Souryal, et al, 1994).

White collar crime is nevertheless an ill defined category of offenses committed by both governments and private corporations. As a general rule, they are crimes committed through negligence, deception, or fraud. In the case of government agencies, they are crimes committed against their own people or against others. Examples include war crimes, political corruption, abuse of power by government agencies, official violence, election fraud, or the systematic involvement in domestic crimes by government agents. In the case of private corporations, these are crimes committed to increase profits illegally. Examples include: the sale of unsafe products, contaminated food, unsafe working conditions, deceptive advertising, taking advantage of the disadvantaged, and garnering extraordinary profits through deception. Needless to say, all such crimes can have a devastating effect on the economic order of the world.

Yet, white collar crimes are, by definition, conspiratorial crimes. They involve agreements to participate in illegitimate schemes. While a formal agreement is not required, most American courts "require an overt act in furtherance of the conspiracy as evidence of a willingness to carry out the planned offense" (Albanese, 1996:17) Regardless of how such conspiracies are formed, however, the *corpus detecti* of all such conspiracies is basically "collective embezzlement." Collective embezzlement has been defined as "the siphoning off of funds or assets from an institution by its management" (Calavita and Pontell, 1991:98). As a result, the public tends to perceive illicit activities committed by corrupt bureaucrats as those that are committed by corrupt corporate managers. Indeed, in a 1979 survey, big businesses in the United States tied with Congress as the "least trusted" institutions from a list of ten major American institutions (Simon, 1996:8).

White collar crimes are, by definition, complicated offenses, despite the fact they are usually committed by a relatively small number of people. They basically require a few well connected, criminally-minded, super-managers (casually known as big fish) who are located in strategic locations. These individuals constitute the "apex" of a network of obscure operatives (casually known as small fish) who surreptitiously "rob" the financial resources of the enterprise through manipulative means. A typical white collar crime begins with a conspiracy to commit collective embezzlement by means of deception, exploitation, or social betrayal. But for the conspiracy to succeed, the participating members may have to commit forgery; to mislead prosecution; to perjure themselves; and to avoid conviction, they may have to obstruct justice by destroying evidence or implicating a wider circle of possibly innocent individuals. In this typical scenario, the public agency or the business involved would be used as a vehicle for perpetuating crime against itself. As such,

white collar crime has also been defined "crimes by the corporation against the corporation."

Examples of the public perception of white collar crimes committed by government institutions include: (1) the belief by about 90 percent of Americans that the United States government was Involved in a conspiracy to murder President Kennedy in 1963; (2) the belief that the United States government was not truthful during the Vietnam war regarding the spraying of more than five million acres in South Vietnam with defoliating chemicals; and (3) the belief that agents of the bureau of Alcohol, Tobacco, and Firearms in 1993 burned the Waco, Texas compound of the Branch Davidian's cult, killing at least 72 members. The agents were later accused of altering their written plans for the assault and lying about these plans (Simon, 1996:5).

Major Examples of White Collar Crime

Examples of white collar crimes committed by individuals in high government positions include: (1) House Speaker Jim Wright resigned in 1989 after being accused of 69 ethics charges including the use of hidden campaign contributions and falsifying incomes received from the selling of a book he wrote; (2) Congressman Dan Rostenkowski was convicted and sentenced to prison in 1996 for engaging in corrupt activities spanning three decades. Rostenkowski's crimes included hiring "ghost employees" who paid him kickbacks, converting to personal use large funds intended to pay for official mailings, and using public funds as personal gifts for friends and families (*The Houston Chronicle*, April 10, 1996); and (3) Ronald Brown, the former Secretary of Commerce, who until his untimely death in 1996, had been under investigation by a special prosecutor for allegations of bribery and kickbacks.

Examples of white collar crimes committed by corporate executives include: (1) the chief executive officer's of America's tobacco companies allegedly amassed huge profits through exploiting the smoking population of the world (especially the young) by manipulating the levels of nicotine in cigarettes. This manipulation has reportedly caused the addiction and the further exploitation of millions of smokers around the world, particularly in third world countries; (2) over the last 30 years, big industrial corporations were charged with "dumping" toxic waste products into the air, water, and landfills, dangerously polluting cities and communities and causing an estimated 500,000 deaths each year (Simon, 1996:9); and (3) corporations have been willfully marketing products known to be dangerous. For

example, Ford Motor Company sold Pinto cars knowing of their defective gasoline tanks and General Motors substituted Chevrolet engines in thousands of its new Oldsmobiles without informing the customers. American corporations have also admitted making bribes of some $ 750 million to officials in foreign countries without informing their stockholders (Simon, 1996:8).

Public Perceptions of White Collar Crime

Public response to white collar crime has been ambivalent, to say the least. In most cultures, it falls short of expressing the moral indignation usually expressed toward other serious crimes. To a large degree, the world community continues to dismiss white collar crime as the "creation of movies," "figments of the media," or simply "deny that it exists" (Bequai,1994). Even when white collar criminality has been admitted, the public normally reacts with placid indifference; in a sense, justifying the perception that such criminal activities only involve "other people's money" (Calavita and Pontell, 1991).

While such perceptions are grossly misleading, there are explanations for these apathetic views :(1) white collar crimes are too complicated; they involve many high stake players engaging in a multitude of business arrangements and financial systems, obviously, in utmost secrecy; (2) white collar crimes invariably involve high ranking government and corporate officials who have great influence on how the laws are made and administered; (3) most white collar crimes involve the embezzlement of assets that are readily available "somewhere," giving the impression that such assets are "nobody's money." Consequently, the targets of white collar crime are seen as "game" for those who have the smarts, poise, and a sense of adventure to grab them; (4) white collar crimes are well-connected to the "highly respectable culture" of computer technology. They are perpetrated by aggressive whiz kids including computer programmers, operators. hackers, and maintenance personnel; (5) from the media standpoint, white collar crime is no longer considered "news." Reports concerning public and private corruption are too "common;" they no longer interest the citizens, nor do they help sell more newspapers; and (6) white collar crimes have now become global crimes, they are much too powerful to stop or deter. To do something about them, therefore, would require that all nations enter into international agreements to prevent, detect, and prosecute such crimes. Reaching such agreements is obviously easier said than done, because many countries stand to reap huge profits by providing safe havens for such illegal operations.

To make matters even worse, white collar criminals are not punished as severely as blue collar offenders. In the 1930s and 1940s, "although 547 adverse court rulings were made against large corporations, no corporate executives were sentenced to prison" (Schmalleger: 1995: 675). More recent studies show that "about 40% were sentenced to prison versus 549 of non-white crime collar criminals" (Schmalleger: 1995: 675). Even "when prison sentences are imposed, white-collar offenders were sentenced to 29 months on average, versus 50 months for other crimes." Schmallegar explains that for unclear reasons, "our system has seen nothing unjust in slapping an 18-year-old inner-city kid with a 20 year prison system sentence for robbing a bank of a couple of thousand dollars, while putting a white-collar criminal away for just two years in a prison camp for stealing $400 million through fraud" (Schmalleger: 1995: 676). This lenient attitude confirms, to a large degree, the relative immunity white collar criminals enjoy as a result of their class, bias by the courts, indifference by society, or a combination of all.

The Cost of White Collar Crime

The economic impact of white collar crime in America has been staggering. Experts estimate that the "yearly cost of embezzlement and theft in American businesses exceeds by several billions the losses sustained throughout the country from traditional crimes of burglary and robbery" (Bequai,1977:5) Bequai reports that "dishonesty by corporate executives and employees has increased the retail cost of merchandise up to 15 percent, and in the case of one firm, caused shareholders to suffer a paper loss of several hundred million dollars within just a few days" (Bequai, 199: 5). Clinard and Yeager (1980) also report that "the total monetary damage caused by white collar crime is somewhere between $174 billion and $231 billion annually while the economic losses resulting from street crimes are estimated to be about $10 billion annually." Based on these figures, it can be safely stated that white collar crimes have been one of the most financially and socially debilitating crimes. They violate the citizens trust in their socioeconomic system, in their system of government, in their fellow citizens, as well as force society into a gauntlet of economic exploitation. This fact may verify the expression, "more money can be stolen at the point of a fountain pen than at the point of a gun" (Schmalleger, 1995: 675).

Two famous examples of white collar crimes from the banking industry shed more light on the real cost of white collar crime--the Savings and Loan scandal in the United States and the Bank of Credit and Commerce International (BCCI) in the far East. In the former case, it is estimated that $200 billion were needed over the

coming decade to bail out the insolvent saving and loan institutions in addition to another $ 500 billion by the year 2000, most of which must be paid by the American taxpayer (Calavita and Pontell, 1991: 94). In the BCCI case,. the bank assets were seized by regulators in 69 countries, making it the largest fraud case in the history of global banking (Simon, 1996:55). Estimates show that BCCI may have defrauded investors of over $5 billion and possibly as much as $15 billion. In 1991, the Bank was fined $200 million and forbidden from engaging in any US banking activities. Bank officials pleaded guilty to laundering $15 million through their Miami and Tampa subsidiaries and paid a record $14.6 million fine. One of BCCI's officials was the personal banker to General Manual Noriega of Panama, who allegedly was a former agent of the Central Intelligence Agency! Furthermore, the scandal may have instrumentally affected the political careers of Prime Minister John Major of Britain and former CIA Director Robert Gates, both of whom allegedly knew of BCCI illegal activities but did little to stop them (Simon, 1996:55).

Is White Collar Crime a Victimless Crime?

Uninformed observers have popularized the view that white collar crime is a victimless crime. This view is based on the fact that, that unlike street crimes, white collar crime is nonviolent and targets no one in particular. Furthermore, it seldom causes physical fear, requires home security measures, or prompts anyone to carry a firearm. From a rational standpoint, however, the socioeconomic damage that these crimes cause is substantial. They are super predatory crimes that while not victimizing any particular category of people (i.e., young, old, male, female, rich, poor, minority, majority), cannibalize entire populations of unsuspecting citizens and consumers.

Several explanations, however, seem to support the perception of white collar crime as "victimless crimes": (1) citizens tend to consider government decisions exempt from "real" public scrutiny because they are made in the country's national interest. This may, indirectly, condone the view that government is free to act deceptively because of its obligation to protect its interests from competition or unfair trade; (2) citizens seem oblivious to the hidden cost of white collar crime; any increases in the cost of living these crimes may cause is intangible and, to a large extent, go unnoticed; and (3) most citizens (as well as law enforcement officials) are led to believe that given the enormity and complexity of white collar crimes, they are impossible to control, anyway.

Given these perceptions, it is a sad commentary to note that the enforcement measures against white collar crimes (especially in the United States) have been fairly lax and, to a great measure, ineffective. The responsibility of enforcing anti white collar crime laws in the United States is assigned to federal agencies, leaving state and local agencies mostly in the dark. Practically, this responsibility is also delegated to only four federal agencies: the Bureau of Alcohol, Tobacco, and Firearms (ATF), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the Internal Revenue Service (IRS). Nevertheless, these agencies have been continuously suffering from "inadequate resources," "lack of expertise," or "excessive reliance on voluntary compliance" by the businesses they are assigned to regulate (Simon, 1996:119). Not surprisingly, law enforcement experts estimate that in the United States, there may be "as few as 300 qualified police investigators who possess the necessary skills to properly investigate such crimes" (Swanson et al., 1996:604).

The White Collar Crime Debate

Criminologists tend to agree that Sutherland's theory was initially presented as an attempt to reform the discipline of criminology which has long advocated that crime is a mean behavior committed by "low social status" persons. By presenting his theory as a new "discovery," Sutherland warned his colleagues of the failure of criminology to consider more realistic views--that crimes can also be committed by "respectable" and "high social status" individuals. By issuing this warning, Sutherland pointed out both the weaknesses of criminology and redefined its subject matter. Sutherland further explained that as long as traditional criminology continued to rely almost exclusively on low-class samples, criminological theory cannot possibly explain all types of crime (Poveda, 1994:32).

On the other hand, critics of Sutherland's have been numerous, each pointing out one or another shortcoming in his arguments. His severest critics, however, were those with legal training, most notably Paul Tappan and Robert Caldwell, who were also trained sociologists. Richard Quinney was perhaps Sutherland's most friendly critic. The thrust of their criticisms was the assertion that white collar crime is at best a moral theory that falls outside the traditional scope of the criminal law (Poveda:1004: 33). Tappan (1947:276) accused Sutherland of: (1) acting as "a white collar criminologist" himself (Sutherland), by using confusing terms that do not distinguish between criminals and non-criminals; (2) by using personal ethics to create a theory of wrongness that constitutes a gross mutilation of criminological thought; and (3) by creating categories of crime under which

government or corporate officials could be accused of criminal acts when there are no criminal laws forbidding such acts, Sutherland's theory must be seen as unnecessary and immaterial; and (4) by talking about white collar crime in such a way that ignores the fact that government and corporate practices are, as they should be, regulated by professional ethics and values is inappropriate.

Caldwell (1958) criticized Sutherland's theory from another perspective. He asserted that the concept of white collar crime violates the sanctity of criminal law, especially the dictum of "no punishment without crime and no crime without law." And since there were no laws forbidding white collar crime activities, such crimes could not exist. Caldwell suggested that Sutherland confused immoral and unethical practices with criminality, thus infusing undue subjectivity which can be detrimental to the integrity of law. As for Sutherland's categorization of white collar crime, Caldwell argued that it was unnecessary simply because public and business decisions are normally subject to "ordinary, business practices" (Caldwell, 1958:33).

Richard Quinney sought to rectify what he saw as inadequacies in Sutherlands's formulation of white collar crime. He argued that "efforts to distinguish categories of white collar crime or to restrict Sutherland's definition must be taken in order to give the concept more social utility" (Quinney, 1964:285). As a solution, he suggested expanding the concept of white collar crime to include all such violations committed in the course of other occupational activities, even by employees who do not fit the definition of "respectable" or "high social status" offenders (Poveda. 1994:35). The most salient point in Quinney's argument is that the criminalization of any behavior must be based on intrinsic "wrongness," rather than on the characteristics of those who commit such a behavior.

Support for Sutherland's theory, however, continues and the term white collar crime is now an integral part of the literature of criminological theory (see Geis, Meier and Salinger, 1977; Cullun, Maakestad, and Cavender, 1987, Edelhertz and Overcast, 1982; Kramer, 1989; Thornberry, 1975; Wolfgang, Figlio, and; Katz, 1980). Presentations on white collar crime are made regularly at professional meetings of criminologists and sociologists, congressional hearings on the subject are continually held. and legislative plans to regulate white collar crimes are a high priority on the agenda of the US Department of Justice.

Operational Definitions of White Collar Crime

The term white collar crime, we must remember, is not a legal term. Indeed such a definition is so ambiguous it is difficult for criminological researchers to determine

the real targets of crime investigations (Simon, 1996). Such a definition can include just about everything committed by upper class persons that is illegal but nonviolent, involving "traditional notions of deceit, deception, concealment, breach of trust, subterfuge or illegal circumvention" (Simon: 1996: 34). Sociologists and criminologists, have, therefore, recognized a number of operational definitions. For the purposes of this article, two such definitions will be presented:

First, white collar crime as: "crimes committed for the purpose of illegitimate financial gain by means of deception by persons having occupational status during their exercise of government or business endeavors" (Schmalleger:1995: 674).

Second, white collar crime as: "an illegal act or series of acts committed by nonphysical means and by concealment or guile, to obtain assets of money or property, or to obtain business or personal advantage." (McGuire and Adelhertz in Geis and Stotland, 1980:199).

Elements of White Collar Crime

While these two definitions indicate slightly different views of what white collar crimes entail, they nevertheless underscore the five basic elements of the crime:

(1) an effective intent (*mens rea*) to commit a wrong act or to achieve an objective in violation of a law or a public policy;
(2) a disguised act (*actus reus*) by which personal or corporate gain is achieved by illegitimate means;
(3) reliance on deceptive means which take advantage of the ignorance or carelessness of victims;
(4) acting on the basis of authority derived from one's position as a public official or a corporate manager; and
(5) a continuing intent to conceal the violation.

Classification of White Collar Crime

It is important that criminologists and law enforcement officials be able to distinguish between three rather distinct categories of white collar crime. While they may be broad and overlapping, thus lending themselves to various interpretations, the impact of white collar crime must be seen the same. The following are the categories of white collar crime based on their impact on society:

(1) White Collar Crime Activities Directed at Physical Harm.

This category is similar to the activities committed by organized criminals, except for being perpetrated by "respectable and high status" persons. Physical harm, in this category, refers to serious damage to health, damage caused by disease or injury, and death. Examples of physical harm (on the domestic scene) include attempts by pharmaceutical companies to sell medicine with hazardous side effects; by automobile companies to sell cars with potentially dangerous components; by tobacco companies to manipulate nicotine levels in cigarettes to promote addiction to tobacco, especially among the young. Examples of physical harm (on the foreign scene) include the deliberate destruction of civilian targets during the Vietnam war the falsifying of reports by field commanders regarding the destruction of enemy targets by spraying millions of acres in South Vietnam with defoliating chemicals and the execution of more than 40,000 so called enemy agents by the Central Intelligence Agency during the Vietnam war (Simon, 1996:3).

(2) White Collar Crime Activities Directed at Financial Harm.

This category is closely associated with the previous one except from a financial standpoint. Examples include the squabble between President Clinton and Congress in 1995 and 1996 over the size of the national budget causing the federal government to shut down for several days incurring the loss of billions of dollars in wasted productivity; fraud by bank directors and overseers as in the case of the Savings and Loans in the United States and the BCCI in Singapore; and illegal practices by oil companies, utility companies and insurance companies which rob the consumers of basic entitlements by arbitrarily raising the cost of their products and services.

(3) White Collar Crime Activities Directed at Moral Harm.

This category is probably the most devastating one since wide scale white collar crime activities can damage the "moral climate" of society by inspiring distrust, cynicism. and alienation. Also, since persons of wealth and power are culturally held to higher standards, being implicated in white crime activities creates negative role models which can dull the moral fiber of society. Not only do they perpetuate a collective sense of frustration and despair, they promote the attitude "if they can do it, I can do it too." Tax authorities have validated this attitude when they noticed that after exposure of former President Nixon's tax deceits, false reporting of taxes

suddenly increased substantially (Geis, Meier, and Salinger, 1995:84). The most significant case, perhaps, illustrating damage to the moral fiber of a nation is Watergate. The "ghost" of Watergate continues to hold a demoralizing effect on the mental and spiritual well-being of America, even a quarter of a century later. While the events of Watergate were in themselves unimportant, the chain of betrayals including lying, cheating, and stealing associated with the case overwhelmed the American spirit. Polls indicate that as a result of Watergate, public confidence in government has been low, and as one poll in particular reveals, "68 percent of Americans continue to believe that their government lied to them" (Simon, 1996:3).

The Centrality of Social Betrayal in White Collar Crime

The three categories of white collar crime are, in a holistic sense, related. They create a sense of "social betrayal" especially since harm in one category would cause harm in the other two. In the "minds and hearts" of common citizens, it makes little difference whether the harm is physical, financial, or moral, as long as it inflicts the sentiment of "social betrayal."

The concept of social betrayal is embedded in the social foundation of the human race. It identifies the balance of power and restraint endemic in the social contract between the governed and the governors--that government officials cannot lie, cheat, or steal. Inherent in this obligation is the expectation that government officials execute all laws faithfully, without bias or prejudice, fear or favor, malice or ill will, and without causing undue harm to their citizens (Jefferson, *The Declaration Of Independence*, 1776). This perception of social betrayal has always been a powerful force behind national revolutions and social upheavals. It has been behind the rise of Hitler and the fall of Communism. Both Germany and Russia, respectively, were suffering from what were considered acts of social betrayal. In the case of Germany, it was by the Allies scheming against them after World War I, and in the case of Russia, by the Communist dictatorship scheming against their own people for over 70 years.

Central as it may be to the conduct of government, the concept of social betrayal continues to be a vague and emotional subject that can only be measured by its effects on society--social disappointment, anguish, and alienation. These are indicators which change every time society experiences difficult times and can be gauged only on a scale of "seriousness ratings." Such ratings can reflect on how deeply hurt the collective conscience of society is. Ratings are, of course,

influenced by the differences in age, sex, the amount of harm, the characteristics of the victim, the offender, and the kind of relationship between them. For example, the sentiment of social betrayal can be considerably heightened when innocent people die, professional soldiers defect, nuns are murdered, children are molested, or elderly people are robbed.

Seriousness ratings concerning the impact of white collar crime in America have been accurate in two recent events: (1) the sudden and unexplained rise in gas prices by about 27 % during the summertime of 2001 when most Americans travel on vacation, and, (2) the continuing denial by tobacco executives of any knowledge associating the manipulation of nicotine in cigarettes to smoking addiction, especially by the youths. Despite the fact that both cases indicate an assumed high level of "social betrayal," the tobacco case indicates a particularly sinister level of betrayal because of its injurious impact on the unsuspecting young and the irrefutable scientific evidence supporting the accusation.

Computer Crime: The Plague of Modern Technology

The explosive growth of computer crime technology has taken the world by storm. As with any other invention, the spellbinding advance of the computer age has created a new menace; a vastly expanded potential for computer crime.

Yet, as in the case of white collar crime, the concept of computer crime has not yet been well established. Unsurprisingly, therefore, it has been said that in the criminal world there are "fraud, theft, larceny, and computer crime," indicating that computer crimes are intrinsically different from all other types of crime: (Parker. 1983: IX). On the other hand, some experts, see no reason to distinguish between computer crimes and other crimes, since society and the legal profession do not distinguish between crimes related to the use of sewing machines, kitchen appliances, or cameras. This perception, however, is rather fuzzy, since the prominence of any crime should be measured by its high rate of incidence. the amount of damage it can cause, its lack of prevention capability, its criminal leverage, and the ratio between the size of reward it can reap and the amount of effort it takes to commit (Parker: IX). The issue, therefore should not be whether computer crimes are a separate classification, but whether they possess distinct characteristics conducive to more harm.

In response to this question, it should be safe to assume that the misuse of a computer can cause more damage than an ordinary weapon. While it is true that

one can cause mischief with a knife or make obscene calls with a telephone, these devices do not have the potential for abuse as does a computer. People do not store secret data or valuable assets in a telephone, and the damage one can inflict with a knife is usually limited to the perpetrator's strength and reach. Even when damage from computers does not materialize, the potential of misuse can be still significant (Gemignani,1988:61). Interestingly, there are those who believe that computers have democratized white collar crime by creating opportunities or big time crimes that were not available otherwise to the "little criminal" (*Business Week*, April 20, 1981).

Definitions

Before defining the term computer crime, an important distinction must be made between two popular terms, computer abuse and computer crime. Computer abuse refers to any intentional act involving the knowledge of computer technology which allows the perpetrator to make some gain and the victim to suffer some loss (Swanson, et al. 1996:604). Computer crime, on the other hand, are illegal acts for which the knowledge of computer technology is used to commit an offense (Swanson, et al. :604). Most experts, however, tend to use the term to mean a broad range of activities consisting of volitional, nonviolent acts involving the use of a computer.

Having made this important distinction, the term computer crime can be defined as "traditional crimes which acquire a new dimension or order of magnitude through the aid of a computer or abuses which have come into being because of the use of computers" (Gemignani, 1988:56).

General Characteristics of Computer Crime

From a criminological viewpoint, computer crimes cannot fit the conventional categorization of criminological theories (i.e., economic need, conflict theory, social control, or biological makeup). If they fit, at all, they more appropriately fall in the category of opportunity theory. People who commit computer crimes are generally motivated by a different set of assumptions. These are basically:

(1) a low risk of detection;
(2) the absence of control structures that regulate the activity;
(3) an attitude toward moral norms and laws which do not deter this form of activity;

(4) an adequate distance between the perpetrator and the victim; and
(5) a sense of anonymity.
These assumptions will be discussed later in greater detail.

Opportunities for computer crimes have been exploding for two significant reasons; the rapid expansion in the use of computers and the more "hookups" computers now have with communication data bases such as the Social Security Administration and the Internal Revenue Service, on the governmental side, and major banks, stock exchanges, hospitals, universities, and air lines, on the business side.

Furthermore, as mentioned earlier, more and more computers are now being connected to the information superhighway, "giving users legitimate (as well as illegitimate) access to sensitive sources of information" For instance, Molnar (1987:714) reports that a few months ago, electronic and print media gave hours of time and yards of column inches to some teenagers from Plainfield, New Jersey, who purportedly reached Pentagon security and moved a functioning satellite. After further investigation, the computer industry trade paper reported that the young hackers had simply gained access to the Department of Defense telephone numbers, numbers that can be dialed by anyone using a cellular telephone (Molnar 1987:714). The reporting of such highly technical computer related crimes has heightened public awareness of the vulnerabilities of computer systems. This also created, at least in part, the need for more regulatory measures to control illicit computer schemes now appearing on "commercial bulletin board" services all over the world.

The computer industry may also have given rise to new techniques of vandalism which can cause serious implications for persons and businesses who depend on computers (Gemignani, 1988:64). Notorious among these techniques are:

(1) Trojan Horses: This technique involves breaking into a bank's data system and putting out an instruction for all users to change their password. As the users comply, the hacker's program records the new passwords allowing the hacker to any assets he chooses. When such a technique is discovered or suspected, the financial institution must shut down its systems for days in order to find the Trojan Horse and change the passwords of the users.

(2) Salami Techniques: This is an automated technique by which computer criminals can steal assets from bank accounts. Since all banks routinely round down their accounts (to the nearest dollar) to facilitate their accounting procedure,

hackers penetrate the computer system instructing the computer to transfer the round down amounts to an account they control and can thus withdraw the funds they want.

(3) Viruses: A computer virus is a bogus program that is secretly inserted into the software program or into the computer's operating system. The impact of these programs runs from disturbing messages to interfering with the computer's operations causing the destruction of data, electronic confusion, and printing errors (Swanson, et al., 1996:606). Swanson quotes the National Computer Security Association statement indicating that in 1994, virus infections caused a loss of $2.7 billion in the United States including the cost of reconstructing files and lost productivity (Swanson. et al. 1996:606).

(4) Logic Bombs: These are illegal program instructions that cause serious damage to the data center on certain times of day or night. Gemignani (1988) reports a story of a Southern California programmer who was charged with two felony accounts of "malicious intent to damage a computer system." The charges stemmed from a "logic bomb" he allegedly placed in a program he wrote for a customer. The bomb placed a "worm" inside the user's operating system which counted the number of times the program was run. When a certain number was reached, the worm changed the disk's identification code so that the user could no longer reach his own data. Another form of computer vandalism is the practice of placing a destructive program on publicly accessible electronic bulletin boards. These programs are described to the user as performing useful functions, but in reality, contain "logic bombs" (Gemignani, 1988:67).

Factors Influencing Vulnerability to Computer Crime

Several factors influence the vulnerability to computer crimes. They are gleaned here from the US Department of Justice International Summaries (Solarz. 1986).

(1) Complexity and the Volume of Data: This factor refers to the complexity and concentration of data in massive data systems. For example, according to figures supplied by the National Insurance Administration's Automatic Data Processing (ADP) in Sweden (a nation of about 8 million people), the national assistance and subsidy system, contains data on 1.7 million children receiving child subsidy and other payments; 0.2 million persons receiving income subsidies and public assistance; 6.6 million registered insured persons; 1.9 million pensioners; 1.3 million children who are wards of the state; and 6.7 million persons contributing to

the national pension fund. Other centralized data system clusters in Sweden include the centralized banking system (all banks in Sweden share an integrated system allowing transactions to be conducted by customers regardless of the bank in which they hold accounts), the police system, the motor vehicle administration, the tax administration, the post office, and the telephone company. Among all of these clusters, the banking system may be the most complex. since transactions take place electronically, including deposits, withdrawals, loan payment; currency exchange, accounting, and investments.

(2) Anonymity: This is probably one of the strongest elements that characterize the environment within which computer crimes are committed. This environment provides almost total anonymity anywhere the user is located including at the workplace, at home, in a car, on a boat, or in an airplane. Anonymity encourages both the motivation to commit crime and reduces the likelihood of being detected. Furthermore, anonymity can be ensured even in the presence of large numbers of people. In a fully automated environment, anonymity can be almost absolute because of the absence of any other parties who have access to the specific transaction. Furthermore, in an automated environment, the perpetrators may experience a lesser sense of guilt since any tangible evidence to the crime is usually lacking. In a manual environment, by contrast, the operatives can easily watch the physical exchange of the stolen items.

(3) Distance from the Victim: This factor makes it both physically and psychologically easier to commit crime. As opposed to the perpetrators of traditional crime who usually have to face their victims, the geographic distance between computer crime perpetrators and their victims may be thousands of miles away. Indeed the greater the distance, the lesser the feeling of guilt on the part of the perpetrator, since he or she may have very little in common with the victim or is not even aware of their human endeavors and interests.

(4) Window of Risk Time: This factor greatly reduces the risk of committing a computer crime. In carrying out a traditional crime (i.e., robbery, burglary, or theft), one can take minutes or hours during which he/she is normally in a heightened state of risk. In a computer crime, on the other hand, this window of risk is greatly reduced since the transition can be made so quickly by clicking a few buttons on a keyboard without ever being noticed.

(5) System Error: This factor is characteristically significant in committing computer crime. It is associated with the inherent tendency of computers to make innocent errors. It works on the assumption that since innocent errors occur, they

can also be used to mask criminal activity. While most computer errors stem from power data quality, in automated environments poor data quality is often difficult to detect and correct. Nevertheless, computer experts estimate that about 35 % of computer failings are due to human error, 20 % to design error, 30 % to poor instruction, documentation, training, and workplace environmental factors (Solarz, 1986:2).

Cyber Crime

Cyber crime is yet another form of computer crime. The term simply represents a new growth in the industry of computers. While there is no definition of what constitutes a cyber crime, it is generally considered to be "any illegal activity that is committed on the Internet or other global service providers by any computer user. In the United States, citizens have a love affair with the Internet which they compare to the Wild West-- a barren landscape devoid of law and order where undesirables can roam at will.

While efforts to regulate use of the Internet are seriously afoot, the network has been invaded by a rapid increase in cyber violations. Three computer developments may have been behind this phenomenon: (1) the spread of low cost personal computers; (2) the soaring number of students and other "moonlighters" who are "tapping" into data transmission lines; and (3) the large number of employees who access computers through the ubiquitous remote terminals.

Yet, despite this loose definition of cyber crime, such activities fall basically within three identifiable categories:

(1) Financial Crimes: These involve the illegal use of a computer system or any of its peripherals for financial gain or advantage (Bequai,1996:23). Financial gain may be direct, as in the case of stealing assets from a bank, or indirect, as in the case of sabotaging a competitor's data system. The technology used in such a crime is a medium for the offense. The manner in which it is employed distinguishes financial cyber offenses from other traditional crimes (Bequai, 1996:23).

(2) Traditional Crimes: These involve the use of computer technology in the commission of traditional illegal acts. They include old-fashioned crimes such as the sale of pornographic materials, conspiring to commit murder, or killing someone in a hospital by sabotaging his/her life support system (Bequai, 1996:231.

(3) Harassment Crimes: These include a broad range of activities involving the misuse of computers. While gaining a financial advantage is not one of the purposes of such activities, the basic objective is frolicking or harassing victims met on the Internet.

Money Laundering: The Illegitimate Child of White Collar Crime and Computer Crime

An alarming, though logical, outcome of the unholy alliance between white collar crime and computer crime is the illegal industry of money laundering. Given the natural tendency of white collar crimes to expand and the serendipity of computer technology, white collar criminals had to invent the practice of money laundering as a requisite for survival.

The theory of money laundering is deceptively simple. White collar crime yields enormous profits in what is known as "dirty money." But, to legitimately profit of this money, these enormous amounts of cash must be systematically "cleansed" or "sanitized." The term laundering stemmed from the common reference to Mafia-ownedl laundromats since laundromats change dirty clothes into clean clothes by removing grime and dirt and making laundered clothes look clean (Chaikin, 1991:467). By the same token, money laundering is used "to break the paper trail, often by using cash or transferring funds overseas to a tax haven (Chaikin, 1991:467). Laundering creates obstacles to government investigators, tax prosecutors, and private detectives who may be on the tail of white collar criminals. As a result, the lure of white collar crimes increases.

The case of Al Capone, mentioned earlier, is a case in point. He reportedly amassed a fortune of $20 million in ten years through bootlegging and gambling. Yet when Capone was prosecuted in 1931, he was charged only with tax evasion. The conviction of Capone was probably the first lesson white collar criminals learned: money that is not reported to tax authorities cannot be spent or reinvested without great risks of detection and prosecution (Swanson. et al. 1996:526). It logically follows, therefore, that white crime collar criminals must utilize money laundering if they are to stay "in business."

Because of its position as a super-target in the world, the United States has enacted several laws against money laundering. Due to their legal complexity, I will only discuss the more recent statutes, including the far reaching Bank Secrecy Act of

1986. This act requires that all banks operating in the United States and its territories file Currency Transaction Reporting (CTR) with the Internal Revenue Service (IRS) regarding any movement of currency (cash or coin) in excess of $10,000. Aggregate deposits to an account totaling $10,000 or more are also reported. The banks, as a result, are held criminally accountable for the implementation of this act.

Another of the most active money laundering statutes is Title 18 of the United States Code, sections 1956 and 1967. Although section 1957 is potentially a much broader section, there have been relatively fewer prosecutions commenced under the former. The article, therefore, focuses primarily on section 1956 (Strafer, 1989). According to this section, it is a federal crime if:

> *Whoever knowing that the property involved in a financial transition represents the proceeds of some form of unlawful activity, conducts or attempts to conducts such a financial transaction which in fact involves the proceeds of specified unlawful activity*

To violate this section, a defendant must be shown to have:

(1) "conducted or "attempted" to conduct;

(2) a "financial transaction;

(3) property which represents the "proceeds" of a specified unlawful activity;

(4) "known" that the property constitutes "proceeds" of "some" unlawful activity;

(5) the "intent" to promote the carrying on of the specified unlawful activity (Strafer, 1989:162).

Anatomy of Money Laundering

The principal purpose of money laundering is to create a justification for possessing or controlling large assets. Without such a justification, a corrupt bureaucrat or a corrupt corporate manager must explain to the tax authorities or the "anti-corruption board" why he/she is living in an $8 million mansion, owns a $6 million yacht, or why his/her spouse's lifestyle is not commensurate with the family income. To avoid these incriminating questions, white collar criminals have

to launder their illicit profits since unaccountable funds in their possession can attract the attention of tax officials.

Specifically, money laundering is the process of "co-mingling" licit and illicit moneies so that they cannot be separated, thus "preventing the discovery or the introduction of illegal money into the business" (Swanson, et al.: 526). Because most checks and credit card receipts are easy to trace, launderers must locate financial or business institutions such as banks, lending agencies, restaurants, bars, or massage parlors which can take in big amounts of cash. After a given time, these institutions would pay back in legitimate checks or other traceable instruments. If money cannot be traced, the basic assumption is that "prosecutors may be blocked, confiscation of assets may be avoided, and debts may not be recovered" (Chaikin, 1991: 58).

Money can be laundered for either legitimate or illegitimate purposes. Legitimate purposes include concealing the assets from the public, competitors, social, religious, or other institutions. It is not uncommon, for instance, to use laundering to conceal the source of funds in a takeover bid, to hide the beneficial ownership of shares in a company, or to pay off foreign agents in a legal manner. Illegitimate purposes, on the other hand, are utilized precisely to avoid detection by tax authorities, prosecutors, and law enforcement agents. While money laundering has been generally thought to be only practiced by drug traffickers, it is obviously not limited only to them. It is equally common among white collar criminals. organized crime criminals, terrorists, and even traditional criminals if the amounts of money involved are exceptionally large.

Types of Money Laundering

It is virtually impossible to estimate the amount of money laundered by white collar criminals. One credible source, however, is the Financial Action Task, an instrument of the US Department of Treasury. Using a combination of methods, the task force postulated that in the United States, the amount of laundered money reached $300 billion in 1987 (Chaikin:473). A more reliable estimate can also be made from the cash that flows through sample banks. In Miami, for instance, that cash flow went from $89 million in 1971 to $5.96 billion in 1985 (Maingot, 1993:177). Current estimates are certainly expected to be much higher.

Money laundering takes place either in domestic or foreign laundries. In one of the foreign cases investigated by the London based Commonwealth Commercial

Crime unit, an offshore bank in the Caribbean was asked to accept a deposit of $300 million at a commission for a kickback in the amount of 3 %. In other words, the bank was to be paid $9 million for agreeing to merely deposit and launder the money (Chaikin, 1991:473).

Domestic Laundries: by definition, these involve local businesses which can be used as a laundromat. Aside from the morality or immorality of their owners or managers (therefore their willingness to be involved in money laundering schemes), such businesses must be capable of absorbing large volumes of cash. Casinos are a perfect choice because they are a cash intensive business that provide financial services similar to those supplied by banks. Typically, casino customers deposit small denomination bills and are paid out in large $100 bills or in casino checks. This provides an ideal cover for money launderers. Another favorable type of domestic businesses is that which deals in expenses that do not vary with sales volume. A good example are movie theaters. Their pay for rent, electricity, and wages are almost constant, regardless of whether the theaters are full (Swanson, et al.:1995: 526). Another favorable type of domestic business is that which experiences a high rate of spoilage or other loss of goods. Groceries and restaurants make great examples.

In Swanson et.al., the authors explain:

> *Money is introduced into the business and recorded in its general income accounts as if it had been received from customers. Fraudulent invoices for produce or other perishable items are issued to these businesses by companies acting as suppliers. The grocery or restaurant issues checks to these "suppliers" or records the transaction as a cash payment. The undelivered produce or perishable items listed as spoiled and discarded are written off the books. The grocery store or restaurant thus avoids tax liability, and the funds paid to "suppliers" seem legal and may be spent or invested with little risk of discovery* (Swanson: 526)

Foreign Laundries: These are considered easier than domestic laundries since they can absorb greater amounts of cash and their return cycle on the "clean money" is shorter. Foreign laundries, depending on their location, may also be more brazen in their practices for two reasons: (1) they are less likely to be subject to stringent laws and, (2) more likely to have greater influence with the political leaders who run the country. Logistically, much of the money profited by white collar criminals is first deposited through secret numbered bank accounts in

smaller countries such as Liechtenstein, Luxembourg, Panama, the Bahamas, the Netherlands, Antilles, the Grand Cayman Islands, Nauru, Vanutau, and Uruguay. The money is then brought back into the United States as a loan from the laundering bank or from a dummy corporation set up under the laws of the foreign country. Under this arrangement. not only are the illegal funds hidden from the tax authorities and law enforcement agencies, but the interest on the supposed loan from the foreign bank is deducted as a business expense (Swanson, et al.:528).

Putting it All Together: Policy Implications for Detection and Investigation

The role of the police has expanded rapidly in the last 30 years and thereby signifies the increasing complexity of modern societies. To cope with societal change, the police must change at a faster pace. The direction of change, however, is crucial: unlike the yesteryears when effective police forces were characterized by physical strength, weaponry, and the use of torture, the crux of police change today has been in the area of knowledge and technology. To be truly effective, police forces of today must work in a calm and a calculated environment where their priorities are rationally and methodically selected in a scientific manner.

Among the growing dangers which face the police forces (i.e., terrorism, gangs, narcotics), combating white collar crimes and computer crimes have been high on the list of advanced societies. Sadly, however, and despite all of the good intentions of most citizens and government leaders, the law enforcement apparatus is ill suited for this new criminal. Bequqi (1977: 14) argues that the police " lack the training and the will, and find themselves engaged in bickering among themselves, thus serving the interest of the white collar criminal."

There are several reasons why fighting white collar crime and computer crime is so difficult to undertake:

First, low reporting rate. Government agencies as well as financial institutions, consulting firms, and corporations are not too interested in reporting fraud and embezzlement for fear of adverse publicity. Governments, by definition, avoid the appearance of corruption for fear of losing public support since corrupt governments are considered primary subjects to revolutions. By the same token, financial institutions do not want their customers and potential depositors to think they are "untrustworthy" or that they are unable to handle their investments. Ironically, in their attempt not to attract attention to their own economic

corruption, many governments are reluctant to pass laws criminalizing white collar crimes.

Second, complexity of investigation and detection. Unlike street crimes where evidence may be in plain view, white collar crimes are highly technological and are committed by "smart criminals," most of whom are better educated than the police. Furthermore, these crimes are, by necessity, "secretive crimes" which are committed in well guarded offices and homes. Linked by telecommunications and working at inconspicuous terminals, white collar criminals are removed from the controls of the workplace. Consequently, eye witnesses are usually lacking, paper trails are at a minimum, and the chances of catching the perpetrators in the act is almost impossible.

Third, the high potential for police investigations to be stymied. White collar criminals (especially those connected with trafficking drugs) are either influential people themselves, or are well connected to influential political leaders. As a result, law enforcement agencies, especially in non-democratic societies, can be faced with a severe dilemma to "turn their faces" the other away or stand the risk of losing their jobs. Moreover, it is not unusual that white collar crime activities are themselves committed by "higher ups" within the police ranks or by administrators who are entrusted to oversee police operations.

Fourth, the difficulty of finding evidence. In white collar investigations the police are faced by the difficulty of recognizing key evidence of illegitimate activities. This is basically due to the weak training of police. Undoubtedly, judges, prosecutors, and law enforcement officials who are unfamiliar (or unwilling to be familiar) with the serious effects of white collar crime and computer crime will be unable to recognize the interdependent nature of evidence that must be collected in white collar crime investigations.

The following policy implications will be presented in two categories: those related to the investigation process, and those related to the training of investigators. The former will address the environment of the investigation process-- its coordination and effectiveness; the latter to the investigative skills that are necessary to combat white collar crimes.

Specific Implications for Effective Investigation

There are four policy implications in this category. These are:

1- The role of the media. Public awareness should be heightened concerning the culpability of white collar criminals and the enormity of damage such crimes can cause society. Society must first be convinced that white collar crimes are "real crimes," if enforcement measures have any chance to succeed. The mass media is obviously the premier tool that can serve this purpose. It should be effectively utilized to educate the public through exposing the hidden aspects of the problem. Furthermore, political parties and governmental agencies should be involved in the formulation of stern laws criminalizing such crimes. In addition, sociologists, criminologists, and economists should focus on the problem and debate it in their professional meetings, and law enforcement agencies should be reeducated as to the seriousness of these crimes.

2- Computer experts should be hired. It is easier (and less costly) to train a computer expert in the arts of investigation than to train a police officer in computer sciences. Experienced computer investigators are so necessary to the successful investigation of these crimes because they know what to search for, they understand the formidable capacities of advanced computers, and they possess the expertise of not attempting moves that can erase data, short-circuit wiring connections, or destroy hidden evidence.

3- The number of expert investigators should be adequate.. Such expert investigators should be organized in groups best trained to meet the needs for intelligence gathering, the interception of communication, the review of financial statements, the collection of latent evidence, and the counseling of prosecutors in the process of building their cases.

4-Investigators Should be trained in Forensic Accountancy. The training of investigators should be both an ongoing endeavor and of the highest quality. In the United States, this is accomplished through specialized governmental training centers such as the FBI and Secret Service training facilities; The Federal Law Enforcement Training Center, in Glenco, Georgia; and The Law Enforcement Electronic Technology Assistance Program created as a model by Florida's 8th judicial circuit.

5- Cooperation with international agencies should be maximized. In this global world, white collar and computer crimes cannot be effectively defeated without a global strategy of cooperation. White collar crimes and, particularly, money laundering activities must be treated as global problems that require the highest degree of collaboration between all countries. It is self-evident that if some

countries cooperated while others did not, the end result would be the displacement of criminal activities from one country to another. The United Nations, the Organization for Economic Cooperation and Development, the European Community, and the International Criminal Police Organization (INTERPOL) have all been instrumental in coordination and facilitating efforts to fight white collar crimes and money laundering activities. The situation today dictates that unless all nations cooperate in good faith, they will sooner or latter suffer serious damages.

The Imperative of Forensic Accountancy

The term forensic accountancy is a new term in the arsenal of contemporary police training. The term evolved as a natural requisite for combating computer crime and in particular, money laundering. The term presupposes that as criminal investigators can recognize crime scenes in a traditional sense, they should also be able to recognize crime scenes in cyber crimes. Furthermore, as criminal investigators can determine criminal evidence and circumstantial evidence in traditional crimes, they should be equally able to determine the same in cyber crime investigations. Hence, there is the need for police to learn and skillfully practice forensic accountancy.

The fundamentals of forensic accountancy include the use of new methods to investigate cyber crime and money laundering. These methods include sampling, ratio analysis, and flow charts, to discover laundering operations as well as to prosecute the individuals involved in them (Swanson, et al.2000: 447). For instance, by using sampling, the police forensic accountant can randomly determine the number of customers of an establishment used for money laundering as well as a conservative estimate of the amount of money spent by each customer. By the same method, the police forensic accountant can also project how much money is actually received by a suspected enterprise in the ordinary course of operation. If the projected income is materially smaller than that reported to taxing authorities, it is a good indication that the business is being used for money laundering.

Another fundamental concept in forensic accountancy is the use of ratio analyses. Such ratios have been used for many years by accountants, investors, and lending institutions. (Swanson, et al. 2000: 447). According to Swanson, Chamelin and Territo, there are four significant types of rations that can be used by police forensic accountants: (1) liquidity ratios that can indicate the abilty of the

enterprise to satisfy its immediate financial obligations; (2) operation ratios that can indicate the efficiency of the business; (3) profitability ratios that can indicate the effective use of assets and the return of the owner's investment in the business; and (4) leverage ratios that can indicate the extent to which the enterprise is financed by debt. Another important concept used by forensic accountants to discover money laundering involves researching the corporate and ownership structures of both the suspected business and all the companies with which it deals.

It should be emphasized, however, that the most significant talent in forensic accountancy by police is capitalizing on their ability to combine common investigative techniques with advanced accountancy techniques, without sacrificing one or the other. Hence, the need for mature and well-experienced detectives who are also interested in accountancy and are comfortable working with numbers, ratios, and statistical analyses. Such talented individuals should be taught both academically and on the job. University degrees should be offered in forensic accountancy and "computerology." Furthermore, such experts should be exclusively certified as investigation experts in the field of white collar crime.

Institutions for Advanced Training

Toward fluency in forensic accountancy, it may be appropriate to familiarize the reader with one of the most advanced training facilities for forensic accountancy in the United States where police officers can be trained in combating white collar crime, computer crime, and money laundering.

The Financial Fraud's Institute (FFI) in Glenco, Georgia is an agency of the United States government and is operated by the Federal Law Enforcement Training Center (FLETC). The Institute has the responsibility for designing, developing, coordinating, and administering programs devoted to the prevention, detection, investigation, and prosecution of complex financial and computer-related frauds. While FFI offers exclusive training to federal, state, and local law enforcement communities, foreign police personnel can also be trained by bilateral agreement.

The FFI provides investigators with specialty skills and techniques to develop solid prosecutable cases in a wide range of crimes. Included are white collar crimes, illegal tax shelters, complex financial transactions, illegal activities in support of terrorism and criminal conspiracies, and money laundering activities including drug smuggling organizations and other illegal enterprises. The Institute also equips investigators with accounting skills applicable to the successful detection

and prosecution of insurance frauds, electronic funds transfer fraud, and employee embezzlement.

One of the most important programs offered by FFI is the Advanced Financial Fraud Training Program (AFFTP). The program focuses on the critical elements and techniques necessary for the successful investigation and prosecution of complex white collar and financial investigations. Courses include: Contract Fraud; Electronic Sources of Information; Computer Related Investigations; Indicators of Financial Fraud; Financial Institutions; Right to Financial Privacy; Money Laundering; Asset Forfeiture; International Investigations and INTERPOL; Federal Sentencing Guidelines; Civil Litigation; and Conflict of Interest.

Another program offered by FFI is the Basic Seized Computer and Evidence Recovery (BSCER). This program focuses on how computer data is created, modified, and manipulated. Courses include: Named Files; Fragmented Erased Files; Unfragmented Erased Files; Location data in Unlocated Space; Hidden Files and Subdirectories using Camouflage Methods; Locating Unreadable Data; Locating Data Unknowingly Written; and Disguised Data.

Another program offered by FFI is the Domestic Money Laundering Training Program (DMLTP). The subject matter of this program focuses on forensic accountancy money and the techniques used to identify, investigate, and prosecute these violations. Courses include: Financial Accounting, Domestic/International Banking, Money Laundering Statutes; Bank Secrecy Act/Title 31; Asset Forfeitures, Record Analysis, Expert Witnesses; Financial Crimes Enforcement, and Money Laundering Methods and Techniques.

A parallel program to DMLTP is the International Banking And Money Laundering Training Program (IBMLTP). This course addresses trends and current developments concerning international banking and money laundering. Courses include: International Banking Framework, Money Laundering Statues; Finance Tracing Money Through Financial Networks; Tax Havens; Bank Secrecy Act; and of course, INTERPOL.

Conclusions

This article addresses the alarming problem of white collar crime especially when it is associated with computer crime. The product of this alliance is a super crime of mammoth dimensions, the surface of which we have just begun to explore. Given the sophisticated technology known as the "information super-highway," the

world may be witnessing a leviathan criminal phenomenon, never before encountered. If taken to its extreme, white collar criminals in one country could technically invade another country--unless extreme safeguards are in place at all times--by siphoning off its public and private assets anywhere these assets are in the world, causing the country's assured demise.

While white collar crime has been traditionally ascribed to "respectable and high status" persons operating in strategic positions, with the advent of computer technology, the crime now attracts anyone who has the technical knowledge to "hack" and the criminal will to engage in big-time criminal activity. What further complicates the problem is the apparent public apathy toward these crimes, causing unjustified leniency in the criminal laws of most advanced countries and the near absence of any laws in most others. Furthermore, with the unprecedented growth in computer technology, white collar crimes have been transformed into global crimes. This requires that all countries "unite" to effectively deter and prevent such crimes, otherwise the social and economic landscape of the world will be disfigured, especially in the poor countries which would be least likely prepared to protect the small assets they may have.

The war against white collar crimes, however, is far from being lost. Political leaders, legislators, judges, prosecutors, and law enforcement agencies can turn the tide and win the war if their efforts were synchronized in the right direction. Toward that synchrony, society should be made fully aware of the staggering price it is paying, effective laws should be enacted criminalizing all aspects of white collar criminal activities, and penalties should be made as severe as the amount of damage these activities cause. Law enforcement agencies around the world should be reeducated concerning the legal and social implication of these crimes and be totally re-trained in the methods of detection, investigation, and prosecution.

In reference to computer crime, we should acknowledge the golden rule that states that "every technology can be beat by a better technology." Accordingly, the scientific and technological communities should be mobilized to design new technologies capable of protecting society's economic and financial interests. Public and private institutions should exercise more vigilance in the way their communication and data centers are protected. But, above all, institutions should hold their officials, at all levels, accountable by requiring higher ethical standards of performance. After all, it is an almost indisputable fact that white collar crimes, by any name, are essentially greed crimes.

End Notes

Albanese, J. S. 1995. *White collar crime in America*. Prentice Hall: Englewood Cliffs.

Bequai, A., 1977. "The Growing Problem of White Collar Crime." *Police Law Quarterly*, Vol. 6 No. 3, 1997.

Calavita, K. and Pontell, H. 1991. "Other People's Money Revisited: Collective Embezzlement in the Savings and Loan and Insurance Industries." *Social Problems*, Vol. 38. No. 1.

Caldwell, R. 1958. "A Reexamination of the concept of White Collar Crime." *Federal Probation*, Vol. 22.

Chaikin, D. 1991. "Money Laundering: An Investigatory Perspective." *Criminal Law Forum* Vol. 2. No. 3. Rutgers University School of Law: Camden, N.J.

Clinard, M and Yeager, P., 1980. *Corporate Crime*. MacMillan: New York.

Cullen, F., Maakestad, W., and Cavender, G., 1987. *Corporate Crime Under Attack The Ford Pinto Case and Beyond*. Anderson: Cincinnati.

Edelhertz, H. and Overcast. T., eds. 1982. *White Collar Crime An Agenda for Research*. Free Press. New York.

Geis, G., Meier R., and Salinger, L. 1995. *White collar crime* Free Press: New York.

Gemignani, M. 1987. "What is Computer Crime, and Why Should we Care." *University of Arkansas Law Journal*, Vol. 10.

Green, G. 1993. "White Collar Crime and the Study of Embezzlement," *The Annals of the American Academy of Political and Social Science*, Vol. 525.

Holy Quran

Katz, J. 1980. "The Social Movement Against White Collar Crime." In Egon Bittner and Sheldon L. Messinger, eds. *Criminology Review Yearbook*, No. 2. Sage: Beverley Hills.

Kramer, R. 1989. "Criminologists and the Social Movement Against Corporate Crime." *Social Justice.* Vol. 16 (Summer).

Maingot, A. 1993. "Laundering the Gains of the Drug Trade: Miami and Caribbean Tax Havens." *Journal of Inter American Studies and World Affairs.* Vol. 30, No. 7.

McGuire, M.. and Edelhertz H. 1980 "Consumer Abuse of Older Americans: Victimization and Remedial Action in Two Metropolitan Areas" in Geis and Stotland, *White Collar Crime: Theory and Research.* Sage: Beverly Hills, 1980.

Molnar, J 1987, "Putting Computer- Related Crime in Perspective." *Journal of Policy Analysis and Management*, Vol. N4..

Parker, D. 1980. "Computer Related White Collar Crime." In Geis and Stotland. *White Collar Crime.* Sage: Beverly Hills.

Poveda, T. 1994. *Fighting Computer Crime*, Scribner's: New York.

Quinney, R. 1964. "The Study of White Collar Crime: Toward a Reorientation in Theory and Research," in Gies and Meier, eds. *White Collar Crime: Offenses in Business, Politics, and the Professions.* Free Press, New York 1977.

Schmalleger, F. 1995. *Criminal Justice Today*, Prentice Hall. New York. '

Solarz, A. 1986. "International Summaries: A Series of Selected Translations in Law Enforcement and Criminal Justice." *US Department of Justice Publication,* National Institute of Justice.

Souryal, S., Dennis P., and Alobied, A. 1994. "The Penalty of Hand Amputation for Theft in Islamic Justice." *Journal of Criminal Justice*, Vol. 22. No. 4.

Strafer, R. 1989. "Money Laundering: The Crime of the 90 's, *American Criminal Law Review*, Vol. 27 No. 149.

Simon, D. 1996. *Elite Deviance*, Allyan and Bacon: Boston.

Swanson, C., Chamelin, N., and Territo, L. 2000. *Criminal Investigation*, McGraw Hill: New York.

Sutherland, E. 1939 "White Collar Criminality" *American Sociological Review*, Vol. 5.

Tappan, P. 1947. "Who is the Criminal" *American Sociological Review*, Vol. 12.

Wolfgang, M., Figlio, R. and Thornberry, T., 1975. *The Criminology Index*. Elsevier: New York.