

Apoorva Bandopadhyay



Cybercrime

An Introduction

Cybercrime: An Introduction

Cybercrime: An Introduction

Apoorva Bandopadhyay



Published by Vidya Books,
305, Ajit Bhawan,
21 Ansari Road,
Daryaganj, Delhi 110002

Apoorva Bandopadhyay
ISBN: 978-93-5429-185-2

© 2021 Vidya Books

This book contains information obtained from authentic and highly regarded sources. All chapters are published with permission under the Creative Commons Attribution Share Alike License or equivalent. A wide variety of references are listed. Permissions and sources are indicated; for detailed attributions, please refer to the permissions page. Reasonable efforts have been made to publish reliable data and information, but the authors, editors and publisher cannot assume any responsibility for the validity of all materials or the consequences of their use.

Trademark Notice: All trademarks used herein are the property of their respective owners. The use of any trademark in this text does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this book by such owners.

The publisher's policy is to use permanent paper from mills that operate a sustainable forestry policy. Furthermore, the publisher ensures that the text paper and cover boards used have met acceptable environmental accreditation standards.

Contents

Chapter 1	Computer Crime: A Brief History	1
Chapter 2	Understanding Cyber Crime	45
Chapter 3	Global Threat of Economic and Cyber Crime	104
Chapter 4	Cyber Terrorism.....	140
Chapter 5	Hacking	161
Chapter 6	Spam Attacks.....	169
Chapter 7	The Challenges of Fighting Cyber Crime.....	182
Chapter 8	Anti-Cyber Crime Strategies	207
Chapter 9	International Legislative Approaches.....	214
Chapter 10	Legal Response.....	244
Chapter 11	Cyber Crime and Cyber Security	291
Chapter 12	Cyber Crime in India.....	302

Chapter 1

Computer Crime: A Brief History

WHY STUDY HISTORICAL RECORDS

Every field of study and expertise develops a common body of knowledge that distinguishes professionals from amateurs. One element of that body of knowledge is a shared history of significant events that have shaped the development of the field. Newcomers to the field benefit from learning the names and significant events associated with their field so that they can understand references from more senior people in the profession and so that they can put new events and patterns into perspective.

This chapter provides a brief overview of some of the more famous (or notorious) cases of computer crime (including those targeting computers and those mediated through computers) of the last four decades.

OVERVIEW

This chapter will illustrate several general trends from the 1960s through the decade following 2000:

- In the early decades of modern information technology (IT), computer crimes were largely committed by individual disgruntled and dishonest employees.
- Physical damage to computer systems was a prominent threat until the 1980s.
- Criminals often used authorised access to subvert security systems as they modified data for financial gain or destroyed data for revenge.
- Early attacks on telecommunications systems in the

1960s led to subversion of the long-distance phone systems for amusement and for theft of services.

- As telecommunications technology spread throughout the IT world, hobbyists with criminal tendencies learned to penetrate systems and networks.
- Programmers in the 1980s began writing malicious software, including self-replicating Programmes, to interfere with personal computers.
- As the Internet increased access to increasing numbers of systems worldwide, criminals used unauthorised access to poorly protected systems for vandalism, political action and financial gain.
- As the 1990s progressed, financial crime using penetration and subversion of computer systems increased.
- The types of malware shifted during the 1990s, taking advantage of new vulnerabilities and dying out as operating systems were strengthened, only to succumb to new attack vectors.
- Illegitimate applications of e-mail grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent e-mail.

1960S AND 1970S: SABOTAGE

Early computer crimes often involved physical damage to computer systems and subversion of the long-distance telephone networks.

Direct Damage to Computer Centers

In February 1969, the largest student riot in Canada was set off when police were called in to put an end to a student occupation of several floors of the Hall Building. The students had been protesting against a professor accused of racism, and when the police came in, a fire broke out and computer data and university property were destroyed. The damages totalled \$2 million, and 97 people were arrested.

Thomas Whiteside cataloged a litany of early physical attacks on computer systems in the 1960s and 1970s:

- *1968, Olympia, WA:* an IBM 1401 in the state is shot twice by a pistol toting intruder.

- *1970, University of Wisconsin:* bomb kills one and injures three people and destroys \$16 million of computer data stored on site.
- *1970, Fresno State College:* Molotov cocktail causes \$1 million damage to computer system.
- *1970, New York University:* radical students place fire-bombs on top of Atomic Energy Commission computer in attempt to free a jailed Black Panther.
- *1972, Johannesburg, South Africa:* municipal computer dented by four bullets fired through a window.
- *1972, New York:* magnetic core in Honeywell computer attacked by someone with a sharp instrument, causing \$589,000 of damage.
- *1973, Melbourne, Australia:* antiwar protesters shoot American firm's computer with double-barreled shotgun.
- *1974, Charlotte, NC:* Charlotte Liberty Mutual Life Insurance Company computer shot by a frustrated operator.
- *1974, Wright Patterson Air Force Base:* four attempts to sabotage computers, including magnets, loosened wires, and gouges in equipment.
- *1977, Rome:* four terrorists pour gasoline on university computer and burn it to cinders.
- *1978, Vandenburg Air Force Base, California:* a peace activist destroys an unused IBM 3031 using a hammer, a crowbar, a bolt cutter and a cordless power drill as a protest against the NAVSTAR satellite navigation system, claiming it gives the US a first-strike capability.

The incidents of physical abuse of computer systems did not stop as other forms of computer crime increased.

For example, in 2001, NewsScan editors summarised a report from Wired Magazine as follows:

- A survey by British PC maker Novatech, intended to take a lighthearted look at techno-glitches, instead revealed the darker side of computing. One in every four computers has been physically assaulted by its owner, according to the 4,200 respondents.

In April 2003, the National Information Protection Center and Department of Homeland Security reported:

- Nothing brings a network to a halt more easily and quickly than physical damage. Yet as data transmission becomes the lifeblood of Corporate America, most big companies haven't performed due diligence to determine how damage-proof their data lifelines really are. Only 20 per cent of midsize and large companies have seriously sussed out what happens to their data connections after they go beyond the company firewall, says Peter Salus of MatrixNetSystems, a network-optimization company based in Austin, TX.

By the mid-2000s, concerns over the physical security of electronic voting systems had risen to public awareness.

For example,

- A cart of Diebold electronic voting machines was delivered today to the common room of this Berkeley, CA boarding house, which will be a polling place on Tuesday's primary election. The machines are on a cart which is wrapped in plastic wrap (the same as the stuff we use in the kitchen). A few cable locks (bicycle locks, it seems) provide the appearance of physical security, but they aren't threaded through each machine. Moreover, someone fiddling with the cable locks, I am told, announced after less than a minute of fiddling that he had found the three-digit combination to be the same small integer repeated three times.

1970-1972: Albert the Saboteur

One of the most instructive early cases of computer sabotage occurred at the National Farmers Union Service Corporation of Denver, where a Burroughs B3500 computer suffered 56 disk head crashes in the 2 years from 1970 to 1972. Down time was as long as 24 hours per crash, with an average of 8 hours per incident. Burroughs experts were flown in from all over the United States at one time or another, and concluded that the crashes must be due to power fluctuations. By the time all the equipment had been repaired and new wiring, motor generators, circuit breakers and power-line

monitors had been installed in the computer room, total expenditures for hardware and construction were over \$500,000 (in 1970 dollars).

Total expenses related to down time and lost business opportunities because of delays in providing management with timely information are not included in this figure. In any case, after all this expense, the crashes continued sporadically as before. By this time, the experts were beginning to wonder about their analysis. For one thing, all the crashes had occurred at night. Could it be sabotage? Surely not! Why, old Albert the night-shift operator had been so helpful over all these years; he had unfailingly called in the crashes at once, gone out for coffee and donuts for the repair crews, and been meticulous in noting the exact times and conditions of each crash. On the other hand, all the crashes had in fact occurred on his shift. Management installed a closed-circuit television (CCTV) camera in the computer room—without informing Albert.

For some days, nothing happened. Then one night, another crash occurred. On the CCTV monitor, security guards saw good ol' Albert open up a disk cabinet and poke his car key into the read/write head solenoid, shorting it out and causing the 57th head crash. The next morning, management confronted Albert with the film of his actions and asked for an explanation. Albert broke down in mingled shame and relief. He confessed to an overpowering urge to shut the computer down. Psychological investigation determined that Albert, who had been allowed to work night shifts for years without a change, had simply become lonely. He arrived just as everyone else was leaving; he left as everyone else was arriving. Hours and days would go by without the slightest human interaction. He never took courses, never participated in committees, never felt involved with others in his company. When the first head crashes occurred—spontaneously—he had been surprised and excited by the arrival of the repair crew. He had felt useful, bustling about, telling them what had happened. When the crashes had become less frequent, he had involuntarily, and almost

unconsciously, re-created the friendly atmosphere of a crisis team. He had destroyed disk drives because he needed company.

IMPERSONATION

Using the insignia and specialised language of officials as part of social engineering has a long history in crime; a dramatization of these techniques is in the popular movie “Catch Me If You Can” about Frank William Abagnale Jr, the teenaged scammer and counterfeiter who pretended to be a pilot, a doctor and a prosecutor before eventually becoming a major contributor to the United States government’s anti-counterfeiting efforts and then founding a major security firm. Several criminals involved in computer-mediated or computer-oriented crime became notorious for using impersonation.

1970: Jerry Neal Schneider

A notorious computer-related crime started in 1970, when teenager Jerry Neal Schneider used Dumpster diving to retrieve printouts from the Pacific Telephone and Telegraph (PT&T) company in Los Angeles. After years of collection, he had enough knowledge of procedures that he was able to impersonate company personnel on the phone. Posing as a freelance magazine writer, he even got a tour of the computerised warehouse and information about ordering procedures.

In June of 1971, he ordered \$30,000 of equipment to be sent to a normal PT&T dropoff point—and promptly stole it and sold it. He eventually had a 6000 square-foot warehouse and 10 employees. He stole over \$1 million of equipment — and sold some of it back to PT&T. He was finally denounced by one of his own disgruntled employees and became a computer security consultant after his prison term.

1980-2003: Kevin Mitnick

Born in 1963, Kevin Mitnick became involved in crime early, using a special punch for bus transfers to get free rides anywhere in the San Fernando Valley in California by the time

he was a young teenager. His own autobiographical comments show him to have been involved in phone phreaking, malicious pranks and breaking into computers at the Digital Equipment Corporation (DEC) using social engineering. In 1981, he and his friend Lewis De Payne used social engineering to gain unauthorised access to an operations center for Pacific Bell; “[T]he juvenile court ordered a diagnostic psychological study of Mitnick and sentenced him to a year’s probation.”

In 1987, he was arrested for breaking into the computers of the Santa Cruz Operation, makers of SCO Unix and sentenced to three years probation. In the summer of 1988, Mitnick and his accomplice and friend Lenny DiCicco cracked the University of Southern California computers again and misappropriated hundreds of Mb of disk space (a lot at the time) to store VAX VMS source files stolen from Digital Equipment Corporation (DEC). Mitnick was arrested by the Federal Bureau of Investigation (FBI) for having stolen the VAX VMS source code. During his trial, he was described as suffering from an impulse-control disorder.

In July 1989, he was sentenced to a year in jail and six months rehabilitation. He later tried to become a private investigator and security specialist. He was generally treated with hostility by the established information security community. In November 1992, Mitnick went underground again when the FBI got a warrant for his arrest on charges of stealing computer time from a phone company. He was located two years later when he made the mistake of leaving insulting messages on the computer and voice-mail systems of a physicist and Internet security expert, Tsutomu Shimomura. Shimomura was so irritated that he helped law enforcement authorities track the fugitive to North Carolina, where Mitnick was arrested in February 1995 and imprisoned pending trial. Mitnick was convicted in federal court for the Central District of California on August 9, 1999 and sentenced to 46 months imprisonment for “four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication.” “Mitnick was previously sentenced by Judge Pfaelzer to an additional 22 months in prison, this for

possessing cloned cellular phones when he was arrested in North Carolina in 1995 and for violating terms of his supervised release imposed after being convicted of an unrelated computer fraud in 1989. He admitted to violating the terms of supervised release by hacking into PacBell voicemail and other systems and to associating with known computer hackers, in this case codefendant Louis De Payne."

Following his release from prison in September 2000, Mitnick was to be on three years parole during which his access to computers was restricted and his profits from writing or speaking about his criminal career were to be turned over to reimburse his victims. Mitnick earned a living on the talk circuit and eventually founded his own security consulting firm. In the years since his release from prison, he has collaborated in writing several books on social engineering. Perhaps his most significant position in the history of computer crime is that he became an icon in the criminal underground. "FREE KEVIN" was a popular component of Web vandalism for many years and Eric Corley, the long-time editor of the criminal-hacking publication *2600: The Hacker Quarterly*, even made a movie, "Freedom Downtime," about what the criminal underground describes as the grossly unfair treatment of Mitnick by the federal government and the news media.

Credit Card Fraud

Credit at local businesses dates back into the undocumented past. In the United States, credit cards appeared in the mid 1920s when gasoline companies began issuing cards that were recognised at stations across the country. In 1950, Frank X. McNamara started the Diners Club, the first credit card company serving multiple types of businesses; the company began the practice of charging a percentage fee for each transaction and also charged its clients a membership fee. The VISA card evolved from the 1951 BankAmericard from the Bank of America and a consortium of California banks established MasterCard shortly thereafter.. American Express stated its card Programme in 1958. Card use

rose and, unsurprisingly, credit card fraud was rampant. Mail theft also became widespread as unscrupulous individuals discovered that envelopes containing credit cards were just like envelopes full of cash. And there was little to stop card companies from sending out cards which customers had never asked for, were not expecting, and could not have known had been stolen until the issuing company began demanding payment for the charges which had been run up. These crimes and other problems stemming from the relentless card-pushing by banks led directly to the passage of the Fair Credit Billing Act of 1974 as well as many other laws designed to protect the consumer. By the mid 1990s, credit card fraud was a rapidly growing problem for consumers and for law enforcement.

A 1997 FBI report stated:

- Around the world, bank card fraud losses to Visa and Master-Card alone have increased from \$110 million in 1980 to an estimated \$1.63 billion in 1995.... The United States has suffered the bulk of these losses-approximately \$875 million for 1995 alone. This is not surprising because 71 percent of all worldwide revolving credit cards in circulation were issued in this country.... Law enforcement authorities continually confront new and complex schemes involving credit card frauds committed against financial institutions and bank card companies. Perpetrators run the gamut from individuals with easy access to credit card information-such as credit agency officials, airline baggage handlers, and mail carriers, both public and private-to organised groups, usually from similar ethnic backgrounds, involved in large-scale card theft, manipulation, and counterfeiting activities. Although current bank card fraud operations are numerous and varied, several schemes account for the majority of the industry's losses by taking advantage of dated technology, customer negligence, and laws peculiar to the industry.

By the late 1990s and in the decade following the year 2000, credit-card fraud was subsumed into the broader category of *identity theft*. Instead of limiting their depredations to running up bills on stolen or forged credit card accounts, thieves, often in organised rings, created entire bogus parallel identities, initiating unpaid bank loans, buying cars with other people's credit, and wreaking havoc with innocent victims' credit ratings, financial situations and even their daily life. Victims of extreme cases lost their ability to obtain mortgages, buy new homes, and accept new jobs. Worse, the burden of proof of innocence fell on the victims in a bitter reversal of the assumption of innocence underlying British Common Law and its offshoot in the Commonwealth and the United States. At the time of this writing, identity theft is the fastest growing form of fraud today.

The National Crime Victimization Survey (NCVS) of the US Department of Justice Bureau of Justice Statistics (BJS) includes surveys dating back to 1973. Currently the random sample includes 77,200 households with 134,000 in all who are contacted every six months and followed for three years. The results for 2005 are available from the BJS Web site as PDF reports and as ZIP files containing spreadsheets for further analysis.

A summary of that research reports that about 6.4M households (5.5 per cent of all the households in the USA) had been affected by some form of identity theft (defined as theft of credit cards, thefts from existing bank accounts, misuse of personal information or multiple types of theft at same time). Losses from credit-card theft averaged \$980 per household; across all type of theft, the average was \$1,620/household; and for misuse of personal information the losses averaged \$4850/household. The most likely victim households were headed by people between 18 and 24 years of age; households with family incomes above \$75,000 were twice as likely to be victimised as those where annual income was less than \$50,000.

Even in the earliest days of telephony, teenaged boys played with the new technology to cause havoc.

In the late 1870s, the new AT&T system in America had to stop using the teenagers as switchboard operators:

- The boys were openly rude to customers. They talked back to subscribers, saucing off, uttering facetious remarks, and generally giving lip. The rascals took Saint Patrick's Day off without permission. And worst of all they played clever tricks with the switchboard plugs: disconnecting calls, crossing lines so that customers found themselves talking to strangers, and so forth.
- This combination of power, technical mastery, and effective anonymity seemed to act like catnip on teenage boys.

2600 Hz

In the late 1950s, AT&T began switching its telephone networks to direct-dial long distance using specific frequency tones to communicate among its switches. Around 1957, a blind seven-year-old child named Josef Engressia with perfect pitch and an emotional fixation on telephones learned to whistle the 2600 Hz pitch that interrupted long-distance telephone calls and allowed him to place a free long-distance call to anywhere in the world. This emotionally-disturbed man eventually renamed himself "Joybubbles and is often described as the founder of phone phreaking – the manipulation of the phone system for unauthorised access to services."

John Draper was in the US Air Force in 1964 when he began helping his colleagues place free phone calls. At the suggestion of Joybubbles, he used the whistles in Cap'n Crunch cereal boxes to generate the 2600 Hz tone and then, calling himself Captain Crunch, went on to create electronic tone synthesisers called *blue boxes*. Apple founders Steve Wozniak and Steve Jobs built blue boxes and perpetrated pranks in the

1970s using the devices such as calling the Vatican while pretending to be Henry Kissinger.

1982-1991: Kevin Poulsen

As the phone system shifted to greater reliance on computers, the border between phreaking and hacking began to blur. One of the important names from the 1980s period of fascination with everything phone-related was Kevin Poulsen.

Kevin Poulsen's autobiographical sketch is shown below:

- Kevin Poulsen first gained notoriety in 1982, when the Los Angeles County District Attorney's Office raided him for gaining unauthorised access to a dozen computers on the ARPANET, the forerunner of the modern Internet. Seventeen years old at the time, he was not charged, and went on to work as a programmer and computer security supervisor for SRI International in Menlo Park, California, then as a network administrator at Sun Microsystems.
- In 1987, Pacific Bell security agents discovered that Poulsen and his friends had been penetrating telephone company computers and buildings. After learning that Poulsen had also worked for a Defence contractor where he'd held a SECRET level security clearance, the FBI began building an espionage case against the hacker.
- Confronted with the prospect of being held without bail, Poulsen became a fugitive. While on the run, he obtained information on the FBI's electronic surveillance methods, and supported himself by hacking into Pacific Bell computers to cheat at radio-station phone-in contests, winning a vacation to Hawaii and a Porsche 944-S2 Cabriolet in the process.
- After surviving two appearances on NBC's *Unsolved Mysteries*, Poulsen was finally captured on April 10th, 1991, in a Van Nuys grocery store, by a Pacific Bell security agent acting on an informant's tip. On December 4th, 1992, Poulsen became the first hacker

to be indicted under U.S., espionage laws when the Justice Department charged him with stealing classified information. (18 U.S.C. 793).

- Poulsen was held without bail while he vigorously fought the espionage charge. The charge was dismissed on March 18th, 1996.
- Poulsen served five years, two months, on a 71 month sentence for the crimes he committed as a fugitive, and the phone hacking that began his case. He was freed June 4th, 1996, and began a three year period of supervised release, barred from owning a computer for the first year, and banned from the Internet for the next year and a half.
- Since, his release, Poulsen has appeared on MSNBC, and on ABC's Nightline, and he was the subject of Jon Littman's flawed book, "The Watchman - the Twisted Life and Crimes of Serial Hacker Kevin Poulsen." His case has earned mention in several computer security and infowar tracts - most of which still report that he broke into military computers and stole classified documents....

After his release from prison, Kevin Poulsen turned to journalism. He became an editor for *SecurityFocus* and then was hired as a Senior Editor at *Wired News*. He is a serious investigative reporter (for example, he broke the story of sexual predators in MySpace) and a frequent contributor to the "Threat Level" blog.

DATA DIDLING

One of the most common forms of computer crime Since, the start of electronic data processing is *data diddling* — illegal or unauthorised data alteration. These changes can occur before and during data input or before output. Data diddling cases have included banks records, payrolls, inventory data, credit records, school transcripts, telephone switch configurations, and virtually all other applications of data processing.

One of the classic early data diddling frauds was the Equity Funding case, which began with computer problems at the Equity Funding Corporation of America, a publicly traded and highly successful firm with a bright idea. The idea was that investors would buy insurance policies from the company and also invest in mutual funds at the same time, with profits to be redistributed to clients and to stock-holders. Through the late 1960s, Equity's shares rose dizzyingly in price; there were news magazine stories about this wunderkind of the Los Angeles business community.

The computer problems occurred just before the close of the financial year in 1964. In despair, the head of data processing told the president the bad news; the report would have to be delayed. Nonsense, said the president expansively (in the movie, anyway); simply make up the bottom line to show about \$10,000,000.00 in profits and calculate the other figures so it would come out that way. With trepidation, the DP chief obliged. He seemed to rationalise it with the thought that it was just a temporary expedient, and could be put to rights later anyway in the real financial books. The expected profit didn't materialise, and some months later, it occurred to the executives at Equity that they could keep the stock price high by manufacturing false insurance policies which would make the company look good to investors.

They therefore began inserting false information about nonexistent policy holders into the computerised records used to calculate the financial health of Equity. In time, Equity's corporate staff got even greedier. Not content with jacking up the price of their stock, they decided to sell the policies to other insurance companies via the redistribution system known as re-insurance. Re-insurance companies pay money for policies they buy and spread the risk by selling parts of the liability to other insurance companies. At the end of the first year, the issuing insurance companies have to pay the re-insurers part of the premiums paid in by the policy holders. So in the first year, selling imaginary policies to the re-insurers

brought in large amounts of real cash. However, when it the premiums came due, the Equity crew “killed” imaginary policy holders with heart attacks, car accidents, and, in one memorable case, cancer of the uterus – in a male imaginary policy-holder. By late 1972, the head of DP calculated that by the end of the decade, at this rate, Equity Funding would have insured the entire population of the world.

Its assets would surpass the gross national product of the planet. The president merely insisted that this showed how well the company was doing. The scheme fell apart when an angry operator who had to work overtime told the authorities about shenanigans at Equity. Rumors spread throughout Wall Street and the insurance industry. Within days, the Securities and Exchange Commission had informed the California Insurance Department that they'd received information about the ultimate form of data diddling: tapes were being erased. The officers of the company were arrested, tried, and condemned to prison terms.

1994: Vladimir Levin and the Citibank Heist

In February 1998, Vladimir Levin was convicted to three years in prison by a court in New York City. Levin masterminded a major conspiracy in 1994 in which the gang illegally transferred \$12M in assets from Citibank to a number of international bank accounts. The crime was spotted after the first \$400,000 were stolen in July 1994 and Citibank cooperated with the FBI and Interpol to track down the criminals. Levin was also ordered to pay back \$240,000, the amount he actually managed to withdraw before he was arrested. The incident led to Citibank's hiring of Stephen R. Katz as the banking industry's first Chief Information Security Officer (CISO).

SALAMI FRAUD

In the salami technique, criminals steal money or resources a bit at a time. Two different etymologies are circulating about the origins of this term. One school of security specialists claim that it refers to slicing the data thin—like a salami. Others

argue that it means building up a significant object or amount from tiny scraps—like a salami. There were documented cases of salami frauds in the 1970s and 1980s, but one of the more striking incidents came to light in January 1993, when four executives of a Value Rent-a-Car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing Programme to add five extra gallons to the actual gas tank capacity of their vehicles.

From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from \$2 to \$15 per customer—rather thick slices of salami but nonetheless difficult for the victims to detect. Unfortunately, one would guess, salami attacks are *designed* to be difficult to detect. The only hope is that random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery. As any accountant will warn, even a tiny error must be tracked down, since it may indicate a much larger problem. For example, Cliff Stoll's famous adventures tracking down spies in the Internet began with an unexplained \$0.75 discrepancy between two different resource accounting systems on UNIX computers at the Keck Observatory of the Lawrence Berkeley Laboratories. Stoll's determination to understand how the problem could have occurred revealed an unknown user; investigation led to the discovery that resource-accounting records were being modified to remove evidence of system use. The rest of the story is told in *The Cuckoo's Egg*.

LOGIC BOMBS

A logic bomb is a Programme which has deliberately been written or modified to produce results when certain conditions are met that are unexpected and unauthorised by legitimate users or owners of the software. Logic bombs may be within standalone Programmes or they may be part of worms (Programmes that hide their existence and spread copies of themselves within a computer systems and through networks)

or viruses (Programmes or code segments which hide within other Programmes and spread copies of themselves). Time bombs are a subclass of logic bombs which “explode” at a certain time. According to a National Security Council employee, the United States government authorised insertion of a time bomb in control software that they knew would be stolen from US sources by the Soviet government to control the Trans-Siberian natural gas pipeline. “The result was the most monumental non-nuclear explosion and fire ever seen from space,” said Thomas C. Reed. The infamous Jerusalem virus (also known as the Friday the 13th virus) of 1988 was a time bomb. It duplicated itself every Friday and on the 13th of the month, causing system slowdown; however, on every Friday the 13th after May 13, 1988, it also corrupted all available disks on the infected systems.

Other examples of notorious time bombs include the following:

- A common PC virus from the 1980s, *Cascade*, made all the characters fall to the last row of the display during the last three months of every year.
- The Michelangelo virus of 1992 was designed to damage hard disk directories on the 6th of March every year.
- In 1992, computer programmer Michael Lauffenburger was fined \$5,000 for leaving a logic bomb at General Dynamics. His intention was to return after his Programme had erased critical data and be paid to fix the problem.

The most famous time bomb of recent years was the Y2K problem. In brief, old Programmes used two-digit year codes that were based on the assumption that they applied to the 20th century. As the 21st century approached, analysts warned of catastrophic consequences if the Programmes were not corrected to use four-digit years or otherwise adapt to the change of century. In the event, the corrective measures worked and there was no disaster. Later analysis showed a positive correlation between investments in Y2K remediation and later profitability.

Computer data can be held for ransom. For example, in 1971, two reels of magnetic tape belonging to a branch of the Bank of America were stolen at Los Angeles International Airport. The thieves demanded money for their return. The owners ignored the threat of destruction because they had adequate backup copies.

Other early cases of extortion involving computers:

- In 1973, a West German computer operator stole 22 tapes and received \$200,000 for their return. The victim did not have adequate backups.
- In 1977, a programmer in the Rotterdam offices of Imperial Chemical Industries, Ltd. (ICI) stole all his employer's tapes, including backups. Luckily, ICI informed Interpol of the extortion attempt. As a result of the company's forthrightness, the thief and an accomplice were arrested in London by officers from Scotland Yard.

In the 1990s, one of the most notorious cases of extortion was the 1999 theft of 300,000 records of customer credit cards from the CD Universe Web site by "Maxus," a 19-year old Russian. He sent an extortion note that read, "Pay me \$100,000 and I'll fix your bugs and forget about your shop forever....or I'll sell your cards and tell about this incident in news." Refused by CD Universe owners, he promptly released 25,000 credit card numbers via a Web site that became so popular with criminals that Maxus had to limit access to one stolen number per visit.

TROJAN HORSES

Trojans are Programmes that pretend to be useful but that either also contain harmful code or are just plain harmful.

The 1988 Flu-Shot Hoax

One of the nastiest tricks played on the shell-shocked world of early microcomputer users was the FLU-SHOT-4 incident of March 1988. With the publicity given to damage

caused by destructive, self-replicating virus Programmes distributed through electronic bulletin board systems (BBSs), it seemed natural that public-spirited programmers would rise to the challenge and provide protective screening. Flu-Shot-3 was a useful Programme for detecting viruses.

Flu-Shot-4 appeared on BBSs and looked just like version 3; however, it actually destroyed critical areas of hard disks and any floppies present when the Programme was run.

The instructions which caused the damage were not present in the Programme file until it was running; this self-modifying code technique makes it especially difficult to identify Trojans by simple inspection of the assembler-level code.

Scrambler, 12-Tricks and PC Cyborg

Other early and notorious PC Trojans from the late 1980s that are still remembered in the industry included:

- The Scrambler (also known as the KEYBGR Trojan), which pretended to be a keyboard driver but actually made a smiley face move randomly around the screen.
- The 12-Tricks Trojan a program for testing the speed of a hard disk but actually caused 12 different kinds of damage (e.g., garbling printer output, slowing screen displays, and formatting the hard disk).
- The PC Cyborg Trojan (or "AIDS Trojan"), which claimed to be an AIDS information program but actually encrypted all directory entries.

1994: Datacomp Hardware Trojan

On November 8, 1994, a correspondent reported to the RISKS Forum Digest that he had been victimised by a curious kind of Trojan:

- I recently purchased an Apple Macintosh computer at a "computer superstore," as separate components - the Apple CPU, and Apple monitor, and a third-party keyboard billed as coming from a company called Sicon.

- This past weekend, while trying to get some text-editing work done, I had to leave the computer alone for a while. Upon returning, I found to my horror that the text “welcome datacomp” had been *inserted into the text I was editing*. I was certain that I hadn’t typed it, and my wife verified that she hadn’t, either. A quick survey showed that the “clipboard” (the repository for information being manipulated via cut/paste operations) wasn’t the source of the offending text.
- As usual, the initial reaction was to suspect a virus. Disinfectant, a leading anti-viral application for Macintoshes, gave the system a clean bill of health; furthermore, its descriptions of the known viruses (as of Disinfectant version 3.5, the latest release) did not mention any symptoms similar to my experiences.
- I restarted the system in a fully minimal configuration, launched an editor, and waited. Sure enough, after a (rather long) wait, the text “welcome datacomp” once again appeared, all at once, on its own.

Further investigation revealed that someone had put unauthorised code in the ROM chip used in several brands of keyboard. The only solution was to replace the keyboard. Readers will understand the possible consequences of a keyboard which inserts unauthorised text into, say, source code. Winn Schwartau has coined the word, “chipping” to refer to such unauthorised modification of firmware.

Keylogger Trojans

By the mid 2000s, software and hardware Trojans designed to capture logs of keystrokes and sometimes to transmit those logs via covert Internet connections had become a well-known tool of industrial espionage.

The United States Department of Homeland Security issued a warning in December 2005 that included the following overview:

- According to industry security experts, the biggest security vulnerability facing computer users and networks is e-mail with concealed Trojan Horse

software—destructive Programmes that masquerade as benign applications and embedded links to ostensibly innocent websites that download malicious code. While firewall architecture blocks direct attacks, e-mail provides a vulnerable route into an organization's internal network through which attackers can destroy or steal information.

- Attackers try to circumvent technical blocks to the installation of malicious code by using social engineering—getting computer users to unwittingly take actions that allow the code to be installed and organization data to be compromised.
- The techniques attackers use to install Trojan Horse Programmes through e-mail are widely available, and include forging sender identification, using deceptive subject lines, and embedding malicious code in e-mail attachments.
- Developments in thumb-sized portable storage devices and the emergence of sophisticated keystroke logging software and devices make it easy for attackers to discover and steal massive amounts of information surreptitiously.

The Haephrati Trojan

A case that made the news in the mid-2000s began when Israeli author Amon Jackont was upset to find parts of the manuscript on which he was working posted on the Internet. Then someone tried to steal money from his bank account. Suspicion fell on his stepdaughter's ex-husband, Michael Haephrati. Police discovered a keystroke logger on Jackont's computer. It turned out that Haephrati had also sold spy software to clients; the Trojan was concealed in what appeared to be confidential e-mail. Once installed on the victims' computers, the software sent surveillance data to a server in London, England. Haephrati was detained by UK police and investigations began in Germany and Israel. Twelve people were detailed in Israel; eight others were under house arrest. Suspects included private investigators and top executives from

industrial firms. Victims included Hewlett-Packard, the Ace hardware stores, and a cable-communications company. Michael and Ruth Haephrati were extradited from Britain for trial in Israel on January 31, 2006. They were accused of installing the Trojan horse Programme that activated the keylogger with remote-reporting capabilities. In March 2006, the couple were indicted in Tel Aviv for corporate espionage. They pleaded guilty to the charges and were sentenced to four and two years of jail, respectively, as well as punished with fines. The story did not end there, however.

Two years later, "Four members of the Israeli Modi'in Ezrahi private investigation firm were sentenced on Monday after they were found guilty of using Trojan malware to steal commercially sensitive information from their clients' competitors." The report continues, "Asaf Zlotovsky, a manager at the Modi'in Ezrahi detective firm, was jailed for 19 months. Two other employees, Haim Zissman and Ron Barhoum, were sent to prison for 18 and nine months respectively. The firm's former chief exec, Yitzhak Rett, the victim of an apparent accident when he fell down a stairwell during a break in police questioning back in 2005, escaped a jail sentence under a plea bargaining agreement. Rett was fined 250,000 Israeli Shekels (£36,500) and ordered to serve ten months' probation over his involvement in the scam." However, an article in April 2008 reported that Michael Haephrati "claimed that there was no jail time, and that he was completely free. As a matter of fact he was going to continue to offer his Trojan Horse service but this time he would only work with - law enforcement agencies'."

Hardware Trojans and Information Warfare

In early 2008, a flurry of news stories discussed the dangers of growing reliance on Chinese-manufactured computing components:

- U.S., Defence Department sources say privately that the level of Chinese cyberattacks obliges them to avoid Chinese-origin hardware and software in all classified systems and as many unclassified systems as fiscally

possible. The high threat of Chinese cyberpenetrations into U.S., Defence networks will be magnified as the Pentagon increasingly loses domestic sources of “trusted and classified” microchips.

The discovery of counterfeit Cisco routers worsened concerns about the reliability of Chinese-manufactured network equipment. The FBI, Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP) and the Royal Canadian Mounted Police (RCMP) worked together to track a massive pattern of counterfeit network hardware including Cisco routers; these investigations and seizures raised questions about the reliability and trustworthiness of such equipment, much of which was manufactured in the People's Republic of China.

Although Cisco scientists examined some of the counterfeit equipment and found no back doors, concern was serious enough that government agencies created test chips to challenge quality assurance processes at military contractors:

- In April [2008], the Defence Advanced Research Projects Agency, part of the Defence Department, began distributing chips with hidden Trojan horse circuitry to military contractors participating in an agency Programme, Trusted Integrated Circuits. The goal is to test forensic techniques for finding hidden electronic trap doors, which can be maddeningly elusive. The agency is not yet ready to announce the results of the test, said Jan Walker, a spokeswoman for the agency.

NOTORIOUS WORMS AND VIRUSES

The following sections briefly describe some of the outstanding incidents that newcomers to the field of information assurance will often hear mentioned in discussions of the history of malware.

1970-1990: Early Malware Outbreaks

The ARPANET was the precursor of the Internet. According to several reports,

- Sometime in the early 1970s, the Creeper virus was

detected on ARPANET, a US military computer network which was the forerunner of the modern Internet. Written for the then-popular Tenex operating system, this Programme was able to gain access independently through a modem and copy itself to the remote system. Infected systems displayed the message, -I'M THE CREEPER: CATCH ME IF YOU CAN.'

- Shortly thereafter, the Reaper Programme was anonymously created to delete Creeper. Reaper was a virus: it spread to networked machines and if it located a Creeper virus, Reaper would delete it. Even the participants are unable to say whether Reaper was a response to Creeper, or if it was created by the same person or persons who created Creeper in order to correct their mistake.

By 1981, the Apple II computer was a popular system among hobbyists; the Elk Cloner virus spread via infected floppy disks and is regarded as "the first large-scale computer virus outbreak in history." In 1986, the Brain boot-sector virus was the first IBM PCs malware to spread around the world.

It was created by two brothers from Lahore, Pakistan and included the following text:

- Welcome to the Dungeon (c) 1986 Brain and Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS: this Programme is catching Programme follows after these messages...\$#@ per cent\$@!!

The Lehigh Virus appeared at Lehigh University in Pennsylvania in 1987 and damaged the files of several professors and students. In 1988, the Jerusalem virus, a file infector that reproduced by inserting its code into EXE and COM files, caused a global PD epidemic. The self-encrypting or polymorphic Cascade virus of 1988 confused many naïve users who interpreted the falling symbols on their screen as part of an unexpected screen saver.

On November 2, 1988, the Internet was rocked by the explosive appearance of unauthorised code on systems all over the world. At 17:00 EST on the 2nd of November 1988, Robert T. Morris, a student at Cornell University in Ithaca, New York released a worm into the Internet. By midnight, it had attacked VAX computers running 4 BSD UNIX and SUN Microsystems Sun 3 computers throughout the United States. One of the most interesting aspects of the Worm's progress through the Internet was the almost complete independence of its path from normal geographical constraints.

It sometimes leaped from coast to coast faster than it reached physically neighbouring computer systems. The worm graphically demonstrated that cyberspace has its own geography. The worm often superinfected its hosts, leading to slowdowns in overall processing speed. The first Internet warning ("We are under attack") was posted at 02:38 on the 3rd of November to the TCP-IP list by a scientist at University of California at Berkeley. At 03:34, Andy Sudduth, a friend of Morris' at Harvard, posted a warning message ("There may be a virus loose on the internet") anonymously and included a few comments on how to stop the Worm. Unfortunately, Spafford writes, the Internet was so severely impeded by the Worm that this message was not widely distributed for over 24 hours. By 06:00 on the morning of the 3rd of November, messages were creeping through the Internet with details of how the Worm worked.

The news spread via news groups such as the TCP-IP list, Usenix 4bsd-ucb-fixes, and the Usenet news.announce. important group. Spafford and his friends and colleagues on the Internet collaborated feverishly on providing patches against the Worm. Meanwhile, as word spread of the attack, some systems administrators began cutting their networks out of the Internet. The Defence Communications Agency isolated its Milnet and Arpanet networks from each other around 11:30 on November 3rd. At noon, machines in the science and technology center at the Stanford Research Institute were shut

down. By late on November 4th, a comprehensive set of patches was posted on the Internet to defend systems against the Worm.

That evening, a New York Times reporter told Spafford that the author of the Worm had been found. By November 8th, the Internet seemed to be back to normal. A group of concerned computer scientists met at the National Computer Security Center to study the incident and think about preventing recurrences of such attacks.

Spafford put the incident into perspective with the comment that the affected systems were no more than 5 per cent of the hosts on the Internet. It would be foolish to dismiss Morris' electronic vandalism as a prank or to claim that the Worm alerted managers to weak security on their systems. Nonetheless, it is true that the incident contributed to the establishment of the Computer Emergency Response Team at the Software Engineering Institute of Carnegie-Mellon University.

For these blessings, however, we owe no gratitude to Robert T. Morris. In 1990, Morris was found guilty under the Computer Fraud and Abuse Act of 1986. The maximum penalties included five years in prison, a \$250,000 fine and restitution costs. Morris was ordered to perform 400 hours of community service, sentenced to three years probation, and required to pay \$10,000 in fines.

He was expelled from Cornell University. His lawyers appealed the conviction to the Supreme Court of the United States. Their arguments included lack of evil intent (he didn't mean to cause harm, honest—even though his Worm took extraordinary precautions to conceal itself) and the scandalous behaviour of Cornell University authorities, who had the temerity to search their own electronic mail message system to locate evidence which incriminated Morris. The lawyers also argued that sending a mail message might become a crime if Morris' conviction were upheld.

The Supreme court upheld the decision by declining to hear the appeal. Robert T. Morris eventually became an

Associate Professor in the Electrical Engineering and Computer Science Department of the Massachusetts Institute of Technology and a member of the Computer Science and Artificial Intelligence Laboratory.

Malware in the 1990s

The most significant malware development of the 1990s was the release in July 1995 of the world's first widely-distributed macro-language virus.

The *macro.concept* virus made its appearance in *MS-WORD for Windows* documents. It demonstrated how to use the macro programming language common to many Microsoft products to generate self-reproducing macros that spread from document to document.

Within a few months, clearly destructive versions of this demonstration virus appeared. Macro viruses were a dangerous new development.

As explained in a recent history of viruses and antivirus,

- Putting self-reproducing code in easily- and frequently exchanged files such as documents greatly increased the infectiousness of the viruses
- Virus writers shifted their attention to a much easier programming language than assembly
- E-mail exchanges of infected documents were a far more effective mechanism for virus infection than exchanges of infected Programmes or disks
- “[M]acro viruses were neither platform-specific, nor OS-specific. They were application-based.”

Over the next few years, macro viruses replaced boot sector viruses and file infector viruses as a major type of malicious self-reproducing malware; during that period, additional types of script-based, network worms also increased.

The following table shows the rise and fall of prevalence of macro viruses over the decade from discovery to extinction using data from the WildList archives. The WildList shows malware identified on user systems by at least two virus researchers.

Table. Rise and Fall in Macro Viruses in the WildList 1996-2008.

Year	Macro-viruses	Total Entries	Percentage Macro-virus
1996	1	183	0.6%
1997	27	239	11%
1998	77	258	30%
1999	46	129	36%
2000	108	175	62%
2001	145	228	64%
2002	103	198	52%
2003	68	205	33%
2004	51	261	20%
2005	22	399	6%
2006	19	804	2%
2007	5	797	0.6%
2008	0	590	0.0%

These data are represented in Figure below.

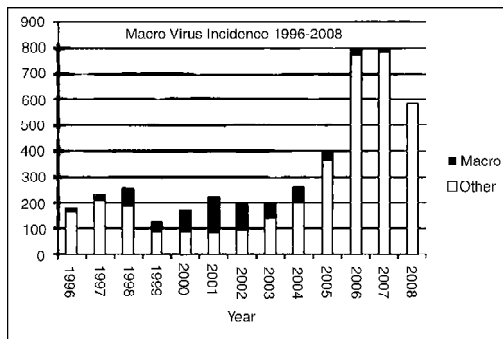


Fig. Macro Virus Incidence 1996-2008.

Roger Thompson summarises the developments in malware in the 1990s as follows:

- By around 2000, macro viruses ceased to be a problem because the new version of MS-Office 2000 included features that blocked macro viruses. The next step in the evolution of malware was the mass mailers like the ILOVEYOU worm and then the network worms. These were easy to write and easy to obfuscate by

varying the text contents, thus defeating signature scanners. These worms spread very quickly until the release of Windows XP Service Pack 2, which forced the Windows Firewall to be on by default. After that extinction-level event, criminals moved onward to creating mass mailers and bots which could spread malware and spam or cause distributed denial-of-service through communication via the trusted Web sites accessed through browsers that created a tunnel through the firewall.

March 1999: Melissa

On Friday 26 March 1999, the CERT/CC received initial reports of a fast-spreading new MS-Word macro virus. "Melissa" was written to infect such documents; once loaded, it uses the victim's MAPI-standard e-mail address book to send copies of itself to the first 50 people on the list. The virus attaches an infected document to an e-mail message with subject line "Subject: Important Message From <name> " where <name> is that of the inadvertent sender. The e-mail message reads, "Here is that document you asked for... don't show anyone else;-)" and includes a MS-Word file as an infected attachment.

The original infected document, "list.doc" was a compilation of URLs for pornographic Web sites. However, as the virus spread it was capable of sending any other infected document created by the victim. Because of this high replication rate, the virus spread faster than any previous virus in history. On many corporate systems, the rapid rate of internal replication saturated e-mail servers with outbound automated junk e-mail.

Initial estimates were in the range of 100,000 downed systems. Anti-virus companies rallied immediately and updates for all the standard products were available within hours of the first notices from CERT/CC. The search for the originator of the Melissa e-mail computer virus/worm began immediately after the outbreak. Initial findings traced the virus to Access Orlando, a Florida Internet Service Provider (ISP), whose

servers were shut down by order of the FBI for forensic examination; the systems were then confiscated. That occurrence was then traced back to Source of Kaos, a free-speech Web site where the virus may have lain dormant for months in a closed but not deleted virus-distributor's pages. Investigators discovered a serial number in the vector document, written with MS-Word; the undocumented serial number helped law enforcement when investigators circulated it on the Net to help track down the perpetrator. The next steps turned to the value-added network AOL, where the virus was released to the public.

The giant ISP's information helped to identify a possible suspect and by the 2nd of April, the FBI arrested David L. Smith (aged 30) of Aberdeen, NJ. Smith apparently panicked when he heard the FBI were on the trail of the Melissa spawner and he threw away his computer — stupidly, into the trash at his own apartment building. Smith was charged with second degree offenses of interruption of public communication, conspiracy to commit the Offence and attempt to commit the Offence, third degree theft of computer service, and third degree damage or wrongful access to computer systems.

If convicted, Smith faced a maximum penalty of \$480,000 in fines and 40 years in prison. On 10 December 1999, Smith pleaded guilty to all federal charges and agreed to every particular of the indictment, including the estimates by the International Computer Security Association of at least \$80M of consequential damages due to the Melissa infections.

May 2000: I LOVE YOU

Starting around May 4, 2000, e-mail users opened messages from familiar correspondents with the subject line "I love you"; many then opened the attachment, LOVE-LETTER-FOR-YOU.txt.vbs which infected the user's e-mail address book and initiated mass mailing of itself to all the contacts. The "Love Bug" was the fastest spreading worm to that time, infecting computers all over the world, starting in Asia, then Europe. On 11 May, Filipino computer science student Onel de Guzman of AMA Computer College in Manila

admitted to authorities that he may “accidentally have launched the destructive Love Bug virus out of youthful exuberance.” He did not admit that he had created the malware himself; however, the name GRAMMERSoft appeared in the computer code of the virus and that was the name of a computer group to which the 23-year-old de Guzman belonged. In September 2000, de Guzman participated in a live chat; he vigorously defended virus-writing and blamed the creators of vulnerable systems for releasing poorly designed software.

He refused to take responsibility for writing the worm. Philippine authorities tried to prosecute de Guzman but had to drop their attempts in August 2000 for lack of sufficient evidence. Due to the lack of computer crime laws at the time, it was impossible for other countries such as the United States to extradite the suspect: international principles of dual criminality require equivalent laws in both jurisdictions before extradition can proceed.

By October 2000, de Guzman had refused to take responsibility for writing the worm and publicly stated, “-I admit I create viruses, but I don’t know if it’s one of mine.... If the source code was given to me, I could look at it and see. Maybe it is somebody else’s, or maybe it was stolen from me.” The I LOVE YOU case was a wake-up call for the international community to think about standardizing computer crime laws around the globe.

SPAM

This section looks solely at a seminal abuse of the USENET in 1994 and trends in spam over the next decade.

1994: The Green Card Lottery Spam

On April 2, 1994, Laurence A. Canter and Martha S. Siegel posted an advertisement for legal services connected to the US government’s Green Card Lottery to over 6,000 USENET groups. Instead of cross-posting their commercial message, they used a script to post a copy of the message separately to every group. The former method would have shown the message to USENET users once; Canter and Siegel’s abuse of the USENET

made their ad show up in every affected group to which users subscribed. Reaction worldwide was massive. Automated cancelbots trolled the USENET deleting the unwanted messages; the attorneys' ISP was so overloaded with e-mail complaints that its servers crashed.

Canter and Siegel were reviled in postings and newspaper articles. Their unsavory backgrounds were posted in discussion groups, including details of disciplinary hearings before the Florida Bar and accusations of dishonesty and unprofessional Behaviour. Unfazed, the couple published a book about how to abuse the Internet using spam and defended their actions in interviews as an expression of freedom of speech; they dismissed critics as "wild-eyed zealots" or as commercial interests intent on controlling the Internet for their own gain. Canter was eventually disbarred in Tennessee, in part for his spamming. He remained unrepentant; in 2002, he spammed 50,000 K-12 teachers with an advertisement for a book whose title he liked so he could harvest payments for referrals from Amazon.

Spam Goes Global

Over the next decade, the incidence of spam grew explosively. By 2007, spam watchers and anti-spam companies reported that around 88 per cent of all e-mail traffic on the Internet was spam. Spammers caused so much irritation that companies developed software and hardware solutions for filtering e-mail by content. Spammers responded by increasing the number of images in their spam, making content filtering more difficult.

At one point, the amount of spam grew 17 per cent between one day and the next as spammers began pumping PDF files into spam pipelines. Botnets spawned through infected zombie machines established rogue SMTP nodes using innocent (and ignorant) PC users' computers and persistent high-speed Internet connections. Spam currently provides a major vector for fraud by deceit, including in particular 4-1-9 advance fee fraud and phishing attacks.

Reducing availability by resource saturation or forced failure of systems has been a technique known to humans ever since, the first proto-human stole someone else's tool. However, in the history of computer crime, a couple of attackers stand out among all the others in the last decade or so: the Unamailer and Mafiaboy.

1996: The Unamailer

In August 1996, someone using the pseudonym "johnny [x]chaotic" [sic] claimed the blame for a massive mail-bombing run based on fraudulently subscribing dozens of victims to hundreds of mailing lists. The denial of service was the result in part of the naïveté of list managers who accepted subscriptions for any e-mail address from any other e-mail address. In a rambling and incoherent letter posted on the Net, (s)he made rude remarks about famous and not so famous people whose capacity to receive meaningful e-mail was obliterated by up to thousands of unwanted messages a day. "The first attack, in August, targeted more than 40 individuals, including Bill Clinton and Newt Gingrich and brought a torrent of complaints from the people who found their names sent as subscribers to some 3,000 E-mail lists." Someone claiming to be the same "Unamailer" (as the news media labeled him or her in reference to the Unabomber) launched a similar mass-subscription mail-bombing run in late December.

This time,

- By comparison to the Christmas attack, even that relatively modest attack sent enough e-mail to the targeted recipients that it effectively halted their computers' ability to process the messages.
- This attack is estimated to involve 10,139 listservs groups, 3 times greater than the one that took place in the summer, also at xchaotic's instigation. If each mailing list in this attack sent the targeted individuals just a modest 10 letters to the subscribers' computer those individuals would receive more than 100,000

messages. If each listing system sent 100 messages — and many do — then the total messages could tally 1,000,000.

In December, the attacker(s) sneered at list administrators for failing to use authentication before allowing subscriptions and wrote that they would continue their attacks until practices changed. Partly as a result of the Unemailer's depredations, list administrators did in fact change their practices — not that anyone thanked Johnny [x]chaotic for his method of persuasion.

2000: Mafiaboy

On February 8, 2000, Yahoo.com suffered a three-hour flood from a distributed denial-of-service (DDoS) attack and lost its capacity to serve Web pages to visitors.

The next day, the same technique was extended to:

- Amazon.com,
- eBay.com,
- Buy.com,
- CNN.com.

Later information also showed that Charles Schwab, the online stock brokerage, had been seriously impeded in serving its customers because of the DDoS. Buy.com managers were particularly disturbed because the attack occurred on the day of their initial public offering. As a result of the attacks, a number of firms formed a consortium to fight DDoS attacks.

Investigation by the RCMP and the FBI located a 15 year old child in west-end Montreal who used a modem to control zombies in his DDoS escapade:

- On April 15, 2000, the RCMP On April 15, 2000, the RCMP arrested a Canadian juvenile known as Mafiaboy for the February 8th DDoS attack on CNN in Atlanta, Georgia. On August 3, 2000, Mafiaboy was charged with 64 additional counts. On January 18, 2001, Mafiaboy appeared before the Montreal Youth Court in Canada and pleaded guilty to 56 counts. These counts included mischief to property in excess of \$5,000 against Internet sites, including CNN.com,

in relation to the February 2000 attacks. The other counts related to unauthorised access to several other Internet sites, including those of several US universities. On September 12, 2001, Mafiaboy appeared before the Montreal Youth Court in Canada and was sentenced to eight months "open custody," one year probation, and restricted use of the Internet.

Mafia Boy's name was not released by Canadian authorities because of Canadian laws protecting juveniles, although several US reporters distributed his identity in their publications. His chief contribution to the history of computer crime was to demonstrate asymmetric warfare in cyberspace. His actions showed that even an ignorant child with little knowledge of computing could use low-tech hardware and tools available to anyone on the Internet to cripple major organizations.

THE HACKER UNDERGROUND OF THE 1980S AND 1990S

Newcomers to the field of information assurance will encounter references to the computer underground in texts, articles and discussions. The following sections provide thumbnail sketches of some of the key groups and events in the shadowy world of criminal hacking (known as *black hats* in contrast with *white hats* who are law enforcement and establishment security experts) and the intermediate range of well-intentioned rebels who use unorthodox means to challenge corporations and governments over what they see as security failings (these people are often called *gray hats*).

1981: Chaos Computer Club

On September 12, 1981, a group of German computer enthusiasts with a strong radical political orientation formed the Chaos Computer Club (CCC) in Hamburg. One of their first achievements was to demonstrate a serious problem in the Bundespost's (German post office) new Bildschirmtext (BTX) interactive videotext service in 1984, not long after the service was announced. The CCC used security flaws in BTX to transferred a sizable amount of money into their own bank

account through a script that ran overnight as a demonstration to the press (returning the money publicly). After the Legion of Underground (LoU) announced on the 1st of January 1999 that they would attack and disable the computer systems of the People's Republic of China and of Iraq, a coalition of hacker organizations including the CCC announced opposition to the move.

"We strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of a country, for any reason," the coalition said. "Declaring war against a country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of," the coalition said in the statement.

The CCC has, in general, challenged the general view that "hacker" necessarily means "criminal hacker." Their annual Chaos Communications Conferences have proven to be a site of technology exchange and serious discussion of information security issues. Their continued commitment to the rule of law (except where their own activities are concerned) and their willingness to engage authorities in the courts when necessary has gained them an unusual degree of credibility and acceptance in the information security community as relatively pale-gray hats.

1982: The 414s

One morning in June 1982, a system administrator for a DEC VAX 11/780 minicomputer at the Memorial Sloan-Kettering Cancer Center in Manhattan found his system down. Investigation led to the discovery that he and dozens of other systems around the country were being hacked by Milwaukee-area teenagers and others aged 15 to 22.

The youths called themselves the 414s after the Milwaukee area code.

- Using home computers connected to ordinary telephone lines, they had been breaking into computers across the U.S., and Canada, including one at a bank in Los Angeles, another at a cement

company in Montreal and, ominously, an unclassified computer at a nuclear weapons laboratory in Los Alamos, [New Mexico].

In March 1984, "two members of Milwaukee's 414 Gang... pleaded guilty to misdemeanor charges of making obscene or harassing phone calls. Maximum sentence for each charge: six months in jail and a \$500 fine."

1984: Cult of the Dead Cow

Another influential criminal-hacker group is the Cult of the Dead Cow (cDc), which used to sport amusing (although intentionally offensive to some) cartoons such as that of a crucified cow. The cDc was noted for its consistent use of humor and parody; for example, "Swamp Rat's" 1985 article on building "The infamous... GERBIL FEED BOMB" included instructions such as "Light the fuse if you put one in. If you dropped a match into it, then go to the nearest phone, dial - 911' and tell the nice people that you have a large number of glass shards embedded in your lower body. An ambulance should be there soon."

The cDc became important proponents of hactivism in the 1990s – the use of criminal hacking techniques for political purposes. They also released a number of hacking tools, of which Back Orifice (BO) and especially Back Orifice 2000 (BO2K) were notorious examples. BO2K was ostensibly a remote administration tool but was in fact a Trojan that ran in stealth mode and allowed remote control of infected machines. Some observers felt that presenting BO2K as a legitimate tool was another instance of cDc's satirical bent: the idea that anyone would consider software written by criminal hackers as a trustworthy administration tool struck them as ludicrous.

1984: 2600: The Hacker Quarterly

Eric Corley founded *2600: The Hacker Quarterly* in 1984. This publication has become a standard bearer for proponents of criminal hacking. The magazine has published a steady stream of explanations of how to exploit specific vulnerabilities

in a wide range of operating systems and application environments.

In addition, the editor's political philosophy has influenced more than one generation of black-hat and gray-hat hackers:

- In the worldview of *2600*, the tiny band of technorat brothers (rarely, sisters) are a besieged vanguard of the truly free and honest. The rest of the world is a maelstrom of corporate crime and high-level governmental corruption, occasionally tempered with well-meaning ignorance. To read a few issues in a row is to enter a nightmare akin to Solzhenitsyn's, somewhat tempered by the fact that *2600* is often extremely funny.

1984: Legion of Doom

The DC comics empire created an animated cartoon series called *Super Friends* that appeared in 1973; it starred various DC Comics heroes such as Superman, Aquaman, Wonder Woman and Batman. In a follow-up series called *Challenge of the Super Friends* that ran from 1978 through 1979, the arch enemies of these heroes were a group known as the *Legion of Doom*, which included *Lex Luthor*, archenemy of Superman. A group of phone phreakers who later turned to criminal hacking called themselves the Legion of Doom (LOD); their founder called himself "Lex Luthor." Another major member was Loyd Blankenship ("The Mentor").

Bruce Sterling describes the LOD as an influential hacker underground group of the 1980s and one of the earliest to capitalise on regular publication of their findings of vulnerabilities and exploits in the phone system and then in computer networks:

- LOD members seemed to have an instinctive understanding that the way to real power in the underground lay through covert publicity. LOD were flagrant. Not only was it one of the earliest groups, but the members took pains to widely distribute their illicit knowledge. Some LOD members, like "The Mentor," were close to evangelical about it. *Legion of*

Doom Technical Journal began to show up on boards throughout the underground.

- *LOD Technical Journal* was named in cruel parody of the ancient and honored *AT&T Technical Journal*. The material in these two publications was quite similar -much of it, adopted from public journals and discussions in the telco community. And yet, the predatory attitude of LOD made even its most innocuous data seem deeply sinister; an outrage; a clear and present danger.

In the later 1980s, the LOD actually helped law enforcement on occasion by restraining malicious hackers. One of the best-known members was Chris Goggans, whose handle was "Erik Bloodaxe;" he was also an editor of *Phrack* and later became part of the Masters of Deception (MOD), which was involved in a conflict with LOD in 1990 and 1991 known in hacker circles as "The Great Hacker War." Another well-known hacker who started in LOD and moved to MOD was Mark Abene ("Phiber Optik"), who was eventually imprisoned for a year after pleading guilty in federal court to conspiracy and unauthorised access to federal-interest computers (a violation of 18 USC 1030(a), the Computer Fraud and Abuse Act of 1986). Abene's punishment was the subject of much protest in the hacker community and elsewhere.

1985: Phrack

Phrack began publishing in November 1985. With a new issue every month or two at first, the electronic magazine continued uninterrupted distribution of technical information and rants. The uncensored commentary provided a fascinating glimpse of some of the personalities and world views of its contributors and editors, including Taran King and Craig Neidorf (later to become famous as "Knight Lightning" and for his involvement in an abortive prosecution involving BellSouth documents). For example, *Phrack* published what became known as the "Hacker Manifesto" – held up by criminal hackers as a light unto the nations ("Written almost 15 years ago by The Mentor, this should be taped up next to everyone's

monitor to remind them who we are, this rang true with Hackers, but it now rings truth to the Internet generation.”) but read with skepticism by security professionals.

It read it part,

- This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin Colour, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
- Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
- I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

In the 1990s, publication frequency faltered, falling to once every three to six months until the editors announced the final issue, #63, for August 2005. However, publication resumed under new editorial leadership in May 2007 with issue 64; given that issue 65 did not come out until April 2008, the magazine's heyday is presumably over.

1989: Masters of Deception (MOD)

The Masters of Deception (MOD) were a New York hacker group active from about 1989 through 1992.

Among the most notorious criminal hackers in the group was "Phiber Optik" (Mark Abene, born in 1972), who was unusually visible in the media:

- Phiber Optik in particular was to seize the day in 1990. A devotee of the 2600 circle and stalwart of the New

York hackers' group "Masters of Deception," Phiber Optik was a splendid exemplar of the computer intruder as committed dissident. The eighteen-year-old Optik, a high-school dropout and part-time computer repairman, was young, smart, and ruthlessly obsessive, a sharp-dressing, sharp-talking digital dude who was utterly and airily contemptuous of anyone's rules but his own. By late 1991, Phiber Optik had appeared in Harper's, Esquire, The New York Times, in countless public debates and conventions, even on a television show hosted by Geraldo Rivera.

1990: Operation Sundevil

After two years of investigation, on May 7, 8, and 9, 1990, 150 FBI agents, aided by state and local authorities, raided presumed criminal hacker organizations allegedly involved in credit card abuse and theft of telephone services. They seized 42 computers and 23,000 disks from locations in 14 cities. Targets were principally sites running discussion boards, some of which were classified as "hacker boards." However, two years after the raid, there were only three indictments (resulting in three guilty pleas). Evidence began to accumulate that much of the evidence seized in the raids was useless.

Bruce Sterling spent a year and a half researching the operation and concluded that it was largely a propaganda effort:

- An unprecedented action of great ambition and size, Sundevil's motives can only be described as political. It was a public-relations effort, meant to pass certain messages, meant to make certain situations clear: both in the mind of the general public, and in the minds of various constituencies of the electronic community.
- First — and this motivation was vital — a "message" would be sent from law enforcement to the digital underground. This very message was recited in so many words by Garry M. Jenkins, the Assistant Director of the US Secret Service, at the Sundevil press conference in Phoenix on May 9, 1990, immediately after the raids. In brief, hackers were mistaken in their

foolish belief that they could hide behind the “relative anonymity of their computer terminals.” On the contrary, they should fully understand that state and federal cops were actively patrolling the beat in cyberspace — that they were on the watch everywhere, even in those sleazy and secretive dens of cybernetic vice, the underground boards.

1990: Steve Jackson Games

Two months before the Operation Sundevil raids, but (contrary to popular conflation of the two) in a completely separate operation, a role-playing game company called Steve Jackson Games in Austin, Texas was raided on March 1, 1990. Some of the equipment seized in the raid was returned four weeks later; most but not all was returned four months later. The company nearly went bankrupt as a result of the sequestration of critical resources. Outrage in the computing community spread beyond the underground.

Mitch Kapor, John Barlow and John Gilmore founded the Electronic Frontier Foundation in part because of their outrage over the treatment of Steve Jackson Games:

- We got the attorneys involved, and then we asked them to look into what was going on with a variety of government investigations and prosecutions. We identified a couple of particular legal situations, like Craig Neidorf in Chicago and Steve Jackson Games, where there seemed to us to have been a substantial overstepping of bounds by the government and an infringement on rights of free speech and freedom of the press. We were in the process of deciding how to intervene when we also realised very clearly that we didn't want to be a legal Defence fund as that was too narrow. What was really needed was to somehow improve the discourse about how technology is going to be used by society; we need to do things in the area of public education and policy development.

Steve Jackson Games sued the Secret Service for damages and were awarded \$50,000 in damages and more than \$25,000

in attorney's fees. The case had a lasting effect on how law enforcement officials carried investigations of computer crimes and seizure of electronic evidence.

1992: L0pht Heavy Industries

In 1992, a group of computer enthusiasts arranged to store their spare equipment in some rented space in Boston. They collaborated on analysis of vulnerabilities, especially Microsoft product vulnerabilities, and gained a reputation for contributing serious research to the field and for appearing at security conferences. Their "L0phtCrack" Programme was adopted by many system administrators for testing password files to locate easy-to-guess passwords; members even testified before a Senate Subcommittee on Government Cyber security in 1998 (saying they could take down the Internet in half an hour). Famous handles from the group included "Brian Oblivion," "Kingpin," "Mudge," "Space Rogue," "Stefan von Neumann," "Tan" and "Weld Pond." The group caused ripples in both the underground and aboveground security communities when their company, L0pht Heavy Industries, was purchased by security services firm @stake, Inc. in 2000. @stake was eventually bought by Symantec in 1994.

2004: Shadowcrew

Stealing physical credit cards and creating fake ones are part of the criminal technique called "carding." One of the significant successful investigations and prosecutions of an international credit-card fraud ring of the 2000 decade began with the US Secret Service's *Operation Firewall* in late 2004. The investigators discovered a network of over 4,000 members communicating through the Internet and conspiring to use phishing, spamming, forged identity documents (e.g., fake driver's licenses), creation of fake plastic credit cards, resale of gift cards bought with fake credit cards, fencing of stolen goods via eBay, and interstate or international funds transfers using electronic money such as E-Gold and Web Money.

In October 2004, the Department of Justice (DOJ) indicted 19 of the leaders of Shadowcrew. By November 2005, 12 of

these people had already pleaded guilty to charges of conspiracy and trafficking in stolen credit card numbers with losses of more than \$4M.

In February 2006, Shadowcrew leader Kenneth J. Flury, 41, of Cleveland OH was sentenced to 32 months in prison with 3 years of supervised release and \$300K in restitution to Citibank. In June 2006, co-founder Andrew Mantovani, 24, of Scottsdale AZ was fined \$5K and also received 32 months of prison with 3 years of supervised release. Five other indicted Shadowcrew criminals were sentenced with him. By that time, a total of 18 of 28 indicted suspects had already pleaded guilty.

CONCLUSION

At some point history becomes current events. At the time of writing, the trends we are seeing dimly may become clear with time. As the first decade of the 21st century draws to its close, it seems to many observers that organised crime has become an integral part of the computer-crime scene – and *vice versa*. The Russian criminal underworld has increasingly invested in high-technology forms of fraud and also relies on high-tech communications for marketing of criminal undertakings such as international traffic in drugs, armaments, and slaves. Information warfare has become a real issue as China advances in technology and seeks growing global power. Terrorist groups cannot ignore the power of asymmetric warfare and must be presumed to be planning attacks on critical infrastructures worldwide. As the global communications network spreads throughout the world, governments, corporations and individuals will have to increase their collaboration and vigilance to defeat the growing army of computer criminals of every type.

Chapter 2

Understanding Cyber Crime

INFRASTRUCTURE AND SERVICES

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, Information and Communication Technologies (ICTs) are omnipresent and the trend of digitalisation is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies such as WiMAX and computer systems that are now available for less than 200 USD, many more people in developing countries should have easier access to the Internet and related products and services.

The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for

developing countries. ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements.

In turn, ICT applications may liberate technical and human capacity and enable greater access to basic services. In this regard online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes, is now one of the main threats to further deployment of e-Government and e-Business services.

The costs of Internet services are often also much lower than comparable services outside the network. E-mail services are often available free of charge or cost very little compared to traditional postal services. The online encyclopaedia Wikipedia can be used free of charge, as can hundreds of online hosting services. Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network.

ADVANTAGES AND RISKS

The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the Information Society. This development of the Information Society offers great opportunities. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities (as has happened, for example, in Eastern Europe). Technical developments have improved daily life – for example, online banking and shopping, the use of Mobile Data Services and Voice over Internet Protocol (VoIP) telephony are just some examples of how far the integration of ICTs into our daily lives has advanced.

However, the growth of the Information Society is accompanied by new and serious threats. Essential services such as water and electricity supply now rely on ICTs. Cars, traffic control, elevators, air conditioning and telephones also depend on the smooth functioning of ICTs.

Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. Attacks against information infrastructure and Internet services have already taken place. Online fraud, the dissemination of child pornography and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day.

The financial damage caused by cyber crime is enormous. In 2003 alone, malicious software caused damages of up to 17 billion USD. By some estimates, revenues from cyber crime exceeded USD 100 billion in 2007, outstripping the illegal trade in drugs for the first time. Nearly 60 per cent of businesses in the United States believe that cyber crime is more costly to them than physical crime. These estimates clearly demonstrate the importance of protecting information infrastructures.

INTERNATIONAL DIMENSIONS OF CYBER CRIME

Cyber crime often has an international dimension. E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient or illegal content is stored outside the country. Within cyber crime investigations, a close cooperation between the countries involved is very important. The existing mutual legal assistance agreements are based on formal, complex and often time-consuming procedures.

The setting-up of procedures for quick response to incidents, as well as requests for international cooperation, is therefore vital. A number of countries base their mutual legal assistance regime on the principle of "dual criminality". Investigations on a global level are generally limited to those crimes that are criminalised in all participating countries. Although there are a number of offences that can be prosecuted anywhere in the world, regional differences play an important role. One example is illegal content. The criminalisation of illegal content differs in various countries. Material that can

lawfully be distributed in one country can easily be illegal in another country. The computer technology currently in use is basically the same around the world.

Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardisation, the protocols used in countries on the African continent are the same as those used in the United States. Standardisation enables users around the world to access the same services over the Internet. The question is what effect the harmonisation of global technical standards has on the development of the national criminal law. In terms of illegal content, Internet users can access information from around the world, enabling them to access information available legally abroad, that could be illegal in their own country.

Theoretically, developments arising from technical standardisation go far beyond the globalisation of technology and services and could lead to the harmonisation of national laws. However, as shown by the negotiations over the First Protocol to the Council of Europe Convention on Cyber crime, the principles of national law change much more slowly than technical developments.

Although the Internet may not recognise border controls, there are means to restrict access to certain information. The access provider can generally block certain websites and the service provider that stores a Web site can prevent access to information for those users on the basis of IP-addresses linked to a certain country ("IP-targeting"). Both measures can be circumvented, but are nevertheless instruments that can be used to keep retain territorial differences in a global network. The OpenNet Initiative reports that such kind of censorship is practised by about two dozen countries.

CONSEQUENCES FOR DEVELOPING COUNTRIES

Finding response strategies and solutions to the threat of cyber crime is a major challenge, especially for developing countries. A comprehensive Anti-Cyber crime Strategy

generally contains technical protection measures, as well as legal instruments. The development and implementation of these instruments need time.

Technical protection measures are especially cost-intensive. Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cyber crime are large and far outweigh any initial outlays on technical protection measures and network safeguards. The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection.

The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries.

The development of technical measures to promote cyber security and proper cyber crime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right from the outset will be less expensive. Developing countries need to bring their anti-cyber crime strategies into line with international standards from the outset.

DEFINITIONS OF CYBER CRIME

Most reports, guides or publications on cyber crime begin by defining the term "cyber crime". One common definition describes cyber crime as any activity in which computers or networks are a tool, a target or a place of criminal activity. One example for an international approach is Art. 1.1 of the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism (CISAC) that points out that cyber crime refers to acts in respect to cyber systems. Some

definitions try to take the objectives or intentions into account and define cyber crime more precisely, defining cyber crime as “computer-mediated activities which are either *illegal or considered illicit* by certain parties and which can be conducted *through global electronic networks*”. These more refined descriptions exclude cases where physical hardware is used to commit regular crimes, but they risk excluding crimes that are considered as cyber crime in international agreements such as the “Convention on Cyber crime”.

For example, a person who produces USB -devices containing malicious software that destroy data on computers when the device is connected commits a crime as defined by Art. 4 Council of Europe Convention on Cyber crime. However, the act of deleting data using a physical device to copy malicious code has not been committed through global electronic networks and would not qualify as cyber crime under the narrow definition.

This act would only qualify as cyber crime under a definition based on a broader description, including acts such as illegal data interference. This demonstrates that there are considerable difficulties in defining the term “cyber crime”. The term “cyber crime” is used to describe a range of offences including traditional computer crimes, as well as network crimes.

As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the Stanford Draft Convention and the Convention on Cyber crime, whilst excluding traditional crimes that are just committed using hardware. The fact that there is no single definition of “cyber crime” need not be important, as long as the term is not used as a legal term.

TYOLOGY OF CYBER CRIME

The term “cyber crime” includes a wide variety of crime. Recognised crimes cover a broad range of offences, making it difficult to develop a typology or classification system for cyber crime. An interesting system can be found in the Council of Europe Convention on Cyber crime.

The Convention on Cyber crime distinguishes between four different types of offences:

1. Offences against the confidentiality, integrity and availability of computer data and systems;
2. Computer-related offences;
3. Content-related offences;
4. Copyright-related offences.

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright-related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as 'Cyber terrorism' or 'phishing') cover acts that fall within several categories. Nonetheless, the categories provided by the Convention on Cyber crime serve as a useful basis for discussing the phenomena of cyber crime.

STATISTICAL INDICATORS ON CYBER CRIME OFFENCES

It is difficult to quantify the impact of cyber crime on society. The financial losses caused by cyber crime, as well as the number of offences, are very difficult to estimate. Some sources estimate losses to businesses and institutions in the United States due to cyber crime to be as high as USD 67 billion; however, it is uncertain if the extrapolation of sample survey results is justifiable.

This methodological criticism applies not only to the losses, but also to the number of recognised offences. It is difficult to measure the number of cyber crimes. Since, targets may not always report these offences. Nevertheless, surveys can help in understanding the impact of cyber crime. More relevant than the precise number of cyber crimes in any single year is the trend, which can be found by comparing results

over several years. One example is the United States CSI Computer Crime and Security Survey 2007 that analyses the number of computer-related offences committed, among other trends.

It is based on the responses of 494 computer security practitioners from U.S corporations, government agencies and financial institutions in the US. The survey documents the number of offences reported by respondents between 2000 and 2007. It shows that, Since, 2001, the proportion of respondents who experienced and acknowledged virus attacks or unauthorised access to information (or system penetration) decreased. The survey does not explain why this decrease has occurred.

However, this decline in the number of recognised offences in the mentioned categories is supported by surveys from other institutions (contrary to what reports in the media sometimes suggest). Similar developments are observed by analysing crime statistics – for example, the German crime statistics show that, after a peak in 2004, the number of computer-related offences has reduced to close to the level of 2002.

The statistics on cyber crime are unable to provide reliable information about the scale or extent of offences. The uncertainty about the extent to which offences are reported by targets, as well as the fact that no explanation for the reducing numbers of cyber crimes can be found, render these statistics open to interpretation. At present, there is insufficient evidence for predictions on future trends and developments.

OFFENCES AGAINST THE CONFIDENTIALITY

All offences in this category are directed against (at least) one of the three legal principles of confidentiality, integrity and availability. Unlike crimes that have been covered by criminal law for centuries (such as theft or murder), the computerisation of offences is relatively recent, as computer systems and computer data were only developed around sixty years ago. The effective prosecution of these acts requires that existing criminal

law provisions not only protect tangible items and physical documents from manipulation, but also extend to include these new legal principles. This section gives an overview of the most commonly occurring offences included in this category.

Illegal Access (Hacking, Cracking)

The offence described by “hacking” refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the United States National Aeronautics and Space Administration (NASA), the United States Airforce, Pentagon, Yahoo, Google, Ebay and the German Government.

Examples of hacking offences include:

- Breaking the password of password-protected websites;
- Circumventing password protection on a computer.

Examples of preparatory acts include:

- Use of faulty hardware or software implementation to illegally obtain a password to enter a computer system;
- Setting up “spoofing” websites to make users disclose their passwords;
- Installing hardware and software based keylogging methods (e.g. “keyloggers”) that record every keystroke – and consequently any passwords used on the computer and/or device.

The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities.



Fig. The Graphic Shows a Website that was Hacked. The Offender Modified the First Page to Inform Users of his Successful Attack.

Others act through political motivation (known as “hacktivism”) – one example is a recent incident involving the main United Nations Web site. In most cases, the motivation of the offender is not limited to illicit access to a computer system. Offenders use this access to commit further crimes, such as data espionage, data manipulation or Denial-of-Service (DoS) attacks.

In most cases, illegal access to the computer system is only a vital first step. Many analysts recognise a rising number of attempts to illegally access computer systems, with worldwide over 250 million incidents recorded during the month of August 2007 alone. Three main factors have supported the increasing number of hacking attacks:

Inadequate and Incomplete Protection of Computer Systems

Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access. Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute. The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks.

Development of Software Tools that Automate the Attacks

Recently, software tools are being used to automate attacks. With the help of software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g., through a botnet – s/he can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the

standardised hacking attacks. High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems.

Tools enabling these standardised attacks are widely available over the Internet – some for free, but efficient tools can easily cost several thousand US dollars. One example is a hacking tool that allows the offender to define a range of IP addresses (e.g. from 111.2.0.0 to 111.9.253.253). The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses.

The Growing Role of Private Computers in Hackers' Strategies

Access to a computer system is often not the primary motivation of an attack. Since business computers are generally better protected than private computers, attacks on business computers are more difficult to carry out using pre-configured software tools. Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected.

Further, private computers often contain sensitive information (e.g. credit card and bank account details). Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities. Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognised as a criminal offence in many countries.

Analysis of different approaches to the criminalisation of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalisation of illegal access to grave violations only.

Some provisions criminalise the initial access, while other approaches limit the criminal offence only to those cases where:

- The accessed system is protected by security measures;

- The perpetrator has harmful intentions;
- Data was obtained, modified or damaged.

Other legal systems do not criminalise mere access, but focus on subsequent offences.

Data Espionage

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets more often. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering United States government and military computer systems, obtain secret information and sell this information to agents from the Soviet Union.

Offenders use various techniques to access victims' computers, including:

- Use of software to scan for unprotected ports;
- Use of software to circumvent protection measures;
- Social engineering.

Especially the last approach "social engineering", which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures, is interesting as it not based on technical means. "Social engineering" is never the less highly effective for attacks on well-protected computer systems. It further describes the manipulation of human beings with the intention of gaining access to computer systems.

Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system. For example, "phishing" has recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication. Although the human vulnerability of users opens the door to the risk of scams, it also offers

solutions. Well-educated computer users are not easy victims for offenders. User education is an essential part of any anticrime strategy. The OECD highlights the importance of cryptography for users, as cryptography can help improve data protection. If the person or organisation storing the information uses proper protection measures, cryptographic protection can be more efficient than any physical protection. The success of offenders in obtaining sensitive information is often due to the absence of protection measures.

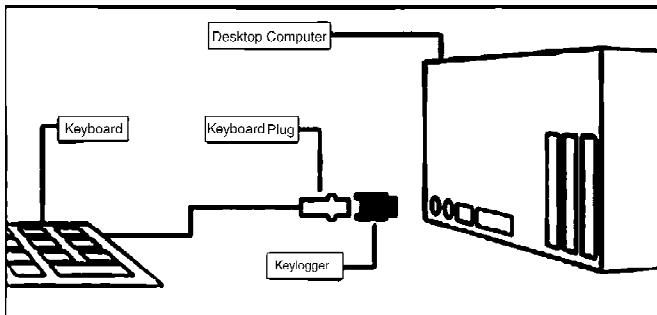


Fig. The Graphic Shows how Hardware keyloggers are Installed. Most such Tools – that Look like Adapters – are Placed between the Keyboard Plug and the Computer. Some of the Latest Models are Included in the Keyboard, so that it is Impossible to find them without Opening the Hardware. Anti-Virus Software Products are not able to Identify Hardware-based Keyloggers.

Although offenders usually target business secrets, data stored on private computers are also increasingly targeted. Private users often store bank account and credit card information on their computer. Offenders can use this information for their own purposes (e.g., bank account details to make money transfers) or sell it to a third party. Credit card records are for example sold for up to USD 60. Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit card information. However, since private computers are generally less protected, data espionage based on private computers is likely to become even more profitable.

There are two approaches to obtaining information, by:

1. Accessing a computer system or data storage device and extracting information;
2. Using manipulation to make users disclose the information or access codes that enable offenders to access information (“phishing”).

Offenders often use computer tools installed on victims’ computers or malicious software called spyware to transmit data to them. Various types of spyware have been discovered over recent years, such as keyloggers. Keyloggers are software tools that record every keystroke typed on an infected computer’s keyboard. Some keyloggers send all recorded information to the offender, as soon as the computer is connected to the Internet. Others perform an initial sort and analysis of the data recorded (e.g. focusing on potential credit card information) to transmit only key data discovered.

Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard. Hardware-based key loggers are more difficult to install and detect, as they require physical access to the computer system. However, classical antispyware and anti-virus software is largely unable to identify them. Apart from the access to computer systems, offenders can obtain data by manipulating the user. Recently, offenders have developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating the user with social engineering techniques. “Phishing” has recently become one of the most important crimes related to cyberspace.

The term “phishing” is used to describe a type of crime that is characterised by attempts to fraudulently acquire sensitive information, such as passwords by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication. Data espionage is another example of a crime that is cleverly aimed at one of the weakest links in computer security: the user. Taking this into consideration clearly demonstrates the risks that are going along with those scams. But it opens the way

for solutions as well. Well-educated computer users will not become an easy victim for the offenders. This highlights the importance of user education as an essential part of any Anti-Cyber crime Strategy. Sensitive information is increasingly being stored in computer systems. It is essential to evaluate whether the technical protection measures undertaken by the users are adequate, or whether law-makers need to establish additional protection by criminalising data espionage.

Illegal Interception

Offenders can intercept communications between users (such as e-mails) or intercept data transfers (when users upload data onto webservers or access web-based external storage media) to record the information exchanged. Offenders can target any communication infrastructure (*e.g.*, fixed lines or wireless) and any Internet service (*e.g.* e-mail, chat or VoIP communications). Most data transfer processes among Internet infrastructure providers or Internet Service Providers are wellprotected and difficult to intercept.

However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable. Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 meters.

Offenders who wish to intercept a data exchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data. To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access (*e.g.*, near bars and hotels). The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point. If users rely on the Access Provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications.

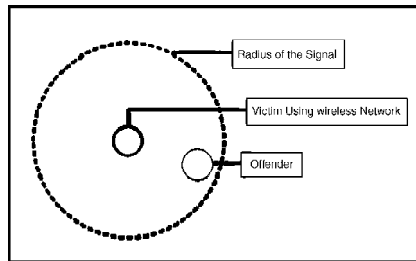


Fig. The Graphic Shows an Attack Scenario Directed against a Computer User Using a Wireless Network Connection. An Offender who Wished to Intercept the Data Sent and Received can Act from any Position Within the Radius of the Signal. Depending on the Wireless Router and its Location, Signals can be Received within a Radius of up to 100 Meter.

The use of fixed lines does not prevent offenders from intercepting communications. Data transmissions passing along a wire emit electromagnetic energy. If offenders use the right equipment, they can detect and record these emissions and may be able to record data transfers between users' computers and the connected system, and also within the computer system. Most countries have moved to protect the use of telecommunication services by criminalising the illegal interception of phone conversations. However, given the growing popularity of IP-based services, law-makers may need to evaluate to what extent similar protection is offered to IP-based services.

Data Interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage.

Offenders can violate the integrity of data and interfere with them by:

- Deleting data;
- Suppressing data;
- Altering data;
- Restricting access to them.

One common example of the deletion of data is the computer virus. Ever since computer technology was first developed, computer viruses have threatened users who failed

to install proper protection. Since then, the number of computer viruses has risen significantly.

Two key recent developments include changes in:

1. The way in which viruses are distributed;
2. The payload.

Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today, most viruses are distributed via the Internet as attachments either to e-mails or to files that users download from the Internet. These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer was estimated to have infected 90 percent of vulnerable computer systems within the first 10 minutes of its distribution. The financial damage caused by virus attacks in 2000 alone was estimated to amount to some 17 billion USD. In 2003 it was still more than 12 billion USD. Most first-generation computer viruses either deleted information or displayed messages.

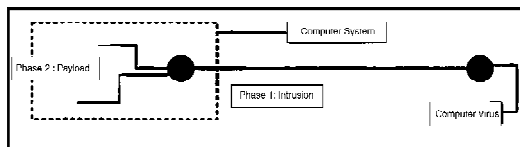


Fig. The Graphic Shows the Functioning of a Computer Virus. After Infecting the Computer System (Phase 1), the Virus Carries out the Programmed Payload (Phase 2). This Could for Example be the Deletion or Encryption of Certain Files.

Recently, payloads have diversified. Modern viruses are able to install back-doors enabling offenders to take remote control of the computer of the victim or encrypt files so that victims are denied access to their own files, until they pay money to receive the key.

System Interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses incorporating Internet services into their production processes,

with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.

Attacks can be carried out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks to the computer system are often far greater than the mere cost of computer hardware.

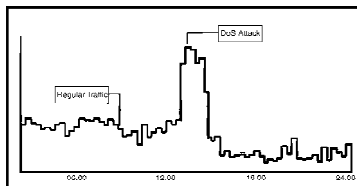


Fig. The Graphic Shows the Number of Access Requests to a Web site During the Normal Operation (black) and During a Denial-of-Service (DoS) Attack. If the Attacked Server is Unable to Handle the Increased Number of Requests, the Attack can Slow down the Web site Response Speed or Disable Service Altogether.

More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include:

- Computer worms;
- Denial-of-Service (DoS) attacks.

Computer worms are a sub-group of malware (like computer viruses). Computer worms are selfreplicating computer programmes that harm the network by initiating multiple data transfer processes.

They can influence computer systems by:

- Depending on the payload of the computer worm, the infection can stop the smooth running operation of the computer system and use system resources to

replicate itself over the Internet.

- The production of network traffic can close down availability of certain services (such as websites).

While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users. By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files.

In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, Ebay and Amazon. As a result, some of the services were not available for several hours and even days. The prosecution of DoS and computer worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic need to criminalise web-based attacks, the question of whether the prevention and prosecution of attacks against critical infrastructure need a separate legislative approach is under discussion.

CONTENT-RELATED OFFENCES

This category covers content that is considered illegal, including child pornography, xenophobic material or insults related to religious symbols. The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies.

The dissemination of xenophobic material is illegal in many European countries, but can be protected by the principle of freedom of speech in the United States. The use of derogatory remarks in respect of the Holy Prophet is criminal in many Arabic countries, but not in some European countries. These legal challenges are complex, as information made

available by one computer user in one country can be accessed from nearly anywhere in the world. If “offenders” create content that is illegal in some countries, but not in the country they are operating from, prosecution of the “offenders” is difficult, or impossible.

There is much lack of agreement regarding the content of material and to what degree specific acts should be criminalised. The different national views and difficulties in prosecuting violations committed outside the territory of an investigating country have contributed to the blocking of certain types of content on the Internet. Where agreement exists on preventing access to websites with illegal content hosted outside the country, states can maintain strict laws, block websites and filter content.

There are various approaches to filter systems. One solution requires access providers to install Programmes analysing the websites being visited and to block websites on a black list. Another solution is the installation of filter software on users’ computer (a useful approach for parents who wish to control the content their children can view, as well as for libraries and public Internet terminals). Attempts to control content on the Internet are not limited to certain types of content that are widely accepted to be illegal. Some countries use filter technology to restrict access to websites addressing political topics. OpenNet Initiative reports that censorship is currently practised by about two dozen countries.

Erotic or Pornographic Material (Excluding Child Pornography)

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including:

- Exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;
- Worldwide access, reaching a significantly larger number of customers than retail shops;
- The Internet is often viewed as an anonymous

medium (often erroneously) – an aspect that consumers of pornography appreciate, in view of prevailing social opinions.

Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.

Besides websites, pornographic material can be distributed through:

- Exchange using file-sharing systems;
- Exchange in closed chat-rooms.

Different countries criminalise erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalisation to cases where minors access this kind of material, seeking to protect minors. Studies indicate that child access to pornographic material could negatively influence their development. To comply with these laws, “adult verification systems” have been developed.

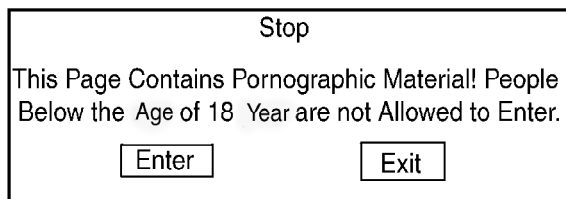


Fig. The Graphic Shows one Approach Used to Prevent Access of Minors to Websites with Pornographic Content. Since this Solution does not Provide Verification of the Answer Given by the User, it is Considered Inadequate in a Number of Countries.

Other countries criminalise any exchange of pornographic material even among adults, without focussing on specific groups (such as minors). For countries that criminalise interaction with pornographic material, preventing access to pornographic material is a challenge. Beyond the Internet, authorities can often detect and prosecute violations of the prohibition of pornographic material. On the Internet, however, as pornographic material is often readily available

on servers outside the country, enforcement is difficult. Even where authorities are able to identify websites containing pornographic material, they may have no powers to enforce removal of offensive content by providers. The principle of *National Sovereignty* does not generally permit a country to carry out investigations within the territory of another country, without permission from local authorities. Even when authorities seek the support of countries where offensive websites are hosted, successful investigation and criminal sanctions may be hindered by the principle of “dual criminality”. To prevent access to pornographic content, countries with exceptionally strict laws are often limited to prevention (such as filter-technology) to limit access to certain websites.

Child Pornography

In contrast to differing views on adult pornography, child pornography is broadly condemned and offences related to child pornography are widely recognised as criminal acts. International organisations are engaged in the fight against online child pornography, with several international legal initiatives including: the 1989 United Nations Convention on the Rights of the Child; the 2003 European Union Council Framework Decision on combating the sexual exploitation of children and child pornography; and the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, among others. Sadly, these initiatives seeking to control the network distribution of pornography have proved little deterrent to perpetrators, who use the Internet to communicate and exchange child pornography.

An increase in bandwidth has supported the exchange of movies and picture archives. Research into the behaviour of child pornography offenders shows that 15 per cent of arrested people with Internet-related child pornography in their possession had more than 1,000 pictures on their computer; 80 per cent had pictures of children between 6-12 years on their computer; 19 per cent had pictures of children younger than the age of 3; and 21 per cent had pictures depicting violence.

Quality	#	Name	Type	Size	Speed	Chat	Bitrate
📁		child pornography, 14yr old girl	dir	2.365 KB	Cable/...	📶	128
📁		15yr, 17yr sex, pamela anderson, porn, movie, illegal, film, hardcore, ha...	dir	8.338 KB	Cable/...	📶	128
📁		PORN, SEX CHILD PORN	dir	5.424 KB	Cable/...	📶	128
📁		cp by MCGAARA (child porn movie)	mpg	10.695...	Cable/...	📶	192
📁		honey school girls (fun, childporn)	mpg	5.176 KB	Cable/...	📶	128
📁		CP 17yr with man	avi	4.124 KB	Cable/...	📶	128
📁		porn, childporn movie	avi	3.291 KB	Cable/...	📶	128
📁		cp, Britney Spears, porn, Pamela Anderson, sex	avi	6.493 KB	Modem	📶	160

Fig. The Graphic Shows the User Interface of a File-sharing Software. After a Request for the Term “Child Pornography” was Submitted, the Software Lists all Files made Available by Users of the File-sharing System that Contain the Term.

The sale of child pornography is highly profitable, with collectors willing to pay great amounts for movies and pictures depicting children in a sexual context. Search engines find such material quickly. Most material is exchanged in password-protected closed forums, which regular users and law enforcement agencies can rarely access. Undercover operations are thus vital in the fight against child pornography. Two key factors in the use of ICTs for the exchange of child pornography pose difficulties for the investigation of these crimes.

The Use of Virtual Currencies and Anonymous Payment

Cash payment enables buyers of certain goods to hide their identity, so cash is dominant in many criminal businesses. The demand for anonymous payments has led to the development of virtual payment systems and virtual currencies enabling anonymous payment. Virtual currencies may not require identification and validation, preventing law enforcement agencies from tracing money-flows back to offenders. Recently, a number of child pornography investigations have succeeded in using traces left by payments to identify offenders. However, where offenders make anonymous payments, it is difficult for offenders to be tracked.

The Use of Encryption Technology

Perpetrators are increasingly encrypting their messages. Law enforcement agencies note that offenders are using

encryption technology to protect information stored on their hard disks, seriously hindering criminal investigations. In addition to a broad criminalisation of acts related to child pornography other approaches such as the implementation of obligations of Internet Service to register users or to block or filter the access to websites related to child pornography are currently discussed.

Racism, Hate Speech, Glorification of Violence

Radical groups use mass communication systems such as the Internet to spread propaganda.

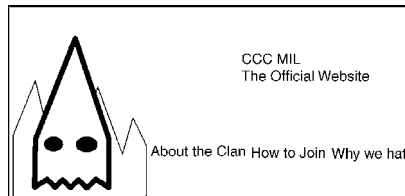


Fig. The Graphic Shows a Web site from a Radical Group. The Internet is Used Intensively by Such Groups to Inform People of their Aims and to Recruit New Members.

Recently, the number of websites offering racist content and hate speech has risen - a study in 2005 suggested a rise of 25 per cent in the number of webpages promoting racial hatred, violence and xenophobia between 2004 and 2005. In 2006, over 6,000 such websites existed on the Internet. Internet distribution offers several advantages to offenders, including lower distribution costs, non-specialist equipment and a global audience. Examples of incitement to hatred websites include websites presenting instructions on how to build bombs. Besides propaganda, the Internet is used to sell certain goods e.g. Nazi-related items such as flags with symbols, uniforms and books, readily available on auction platforms and specialised web-shops. The Internet is also used to send e-mails and newsletters and distribute video clips and television shows through popular archives such as YouTube. Not all countries criminalise these offences. In some countries, such

content may be protected by principles of freedom of speech. Opinions differ as to how far the principle of freedom of expression applies with regard to certain topics, often hindering international investigations. One example of conflict of laws is the case involving the service provider Yahoo! in 2001, when a French court ordered Yahoo! (based in the US) to block the access of French users to Nazi-related material. Based on the First Amendment of the United States Constitution, the sale of such material is legal under United States law. Following the First Amendment, a US court decided that the French order was unenforceable against Yahoo! in the United States. The disparities between countries on these issues were evident during the drafting of the Council of Europe Convention on Cyber crime. The Convention seeks to harmonise cyber crime-related laws to ensure that international investigations are not hindered by conflicts of laws. Not all parties engaged in negotiations could agree on a common position on the criminalisation of the dissemination of xenophobic material, so this entire topic was excluded from the Convention and instead addressed in a separate First Protocol. Otherwise, some countries (including the United States) might have been unable to sign the Convention.

Religious Offences

A growing number of websites present material that is in some countries covered by provisions related to religious offences *e.g.*, anti-religious written statements. Although some material documents objective facts and trends (*e.g.*, decreasing church attendance in Europe), this information may be considered illegal in some jurisdictions. Other examples include the defamation of religions or the publication of cartoons.

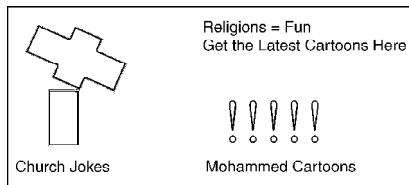


Fig. The Graphic Shows a Website that makes Available Content with a Religious Background, which can be Accessed by Users Worldwide.

The Internet offers advantages for those who wish to debate or deal critically with a subject – people can leave comments, post material or write articles without having to disclose their identity. Many discussion groups are based on the principle of freedom of speech. Freedom of Speech is a key driver behind the Internet's success, with portals that are used specifically for user-generated content.

Whilst it is vital to protect this principle, even in the most liberal countries, conditions and laws govern the application of principles of Freedom of Speech. The differing legal standards on illegal content reflect the challenges of regulating content. Even where the publication of content is covered by provisions relating to Freedom of Speech in the country where the content is available, this material can be accessed from countries with stricter regulations.

The "Cartoon Dispute" in 2005 demonstrated the potential for conflict. The publication of twelve editorial cartoons in the Danish newspaper Jyllands-Posten led to widespread protests across the Muslim world. As with illegal content, the availability of certain information or material is a criminal offence in some countries. The protection of different religions and religious symbols differs from country to country. Some countries criminalise the use of derogatory remarks in respect of the Holy Prophet or the defiling of copies of the Holy Quran, while other countries may adopt a more liberal approach and may not criminalise such acts.

Illegal Gambling and Online Games

Internet games and gambling are one of the fastestgrowing areas in the Internet. Linden Labs, the developer of the online game Second Life, reports that some ten million accounts have been registered.

Reports show that some such games have been used to commit crimes including:

- Exchange and presentation of child pornography;
- Fraud;
- Gambling in online casinos; and
- Libel (e.g. leaving slanderous or libelous messages).

Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling (although compared with revenues from traditional gambling, these estimates are still relatively small). The regulation of gambling over and outside the Internet varies between countries - a loophole that has been exploited by offenders, as well as legal businesses and casinos. The effect of different regulations is evident in Macau. After being returned by Portugal to China in 1999, Macau has become one of the world's biggest gambling destinations. With estimated annual revenues of USD 6.8 billion in 2006, it took the lead from Las Vegas (USD 6.6 billion). Macau's success derives from the fact that gambling is illegal in China and thousands of gamblers travel from Mainland China to Macau to play. The Internet allows people to circumvent gambling restrictions. Online casinos are widely available, most of which are hosted in countries with liberal laws or no regulations on Internet gambling.

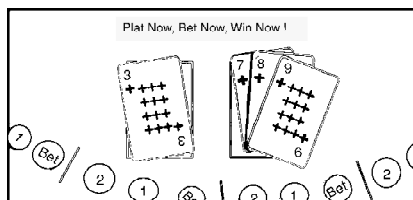


Fig. The Graphic Shows the User Interface of an Online Casino. After a Registration Process and the Transfer of Money the User can Participate in Online Gambling. A Number of Online Casinos Enable the Use of Services Without a Formal Registration Progress.

Users can open accounts online, transfer money and play games of chance. Online casinos can also be used in money-laundering and activities financing terrorism.

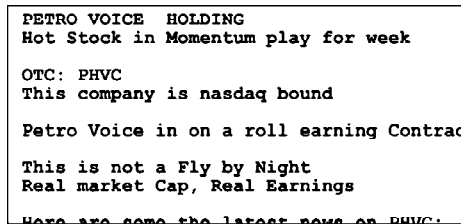
If offenders use online casinos within the laying-phase that do not keep records or are located in countries without money-laundering legislation, it is difficult for law enforcement agencies to determine the origin of funds. It is difficult for countries with gambling restrictions to control the use or activities of online casinos. The Internet is undermining some countries' legal restrictions on access by citizens to online

gambling. There have been several legislative attempts to prevent participation in online gambling: notably, the US Internet Gambling Prohibition Enforcement Act of 2006 seeks to limit illegal online gambling by prosecuting financial services providers if they carry out settlement of transactions associated with illegal gambling.

Libel and False Information

The Internet can be used to spread misinformation, just as easily as information. Websites can present false or defamatory information, especially in forums and chat rooms, where users can post messages without verification by moderators.

Minors are increasingly using web forums and social networking sites where such information can be posted as well. Criminal behaviour can include (for example) the publication of intimate photographs or false information about sexual behaviours. In most cases, offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID. This makes the identification of offenders complicated. Furthermore, there may be no or little regulation of content by forum moderators.



```
PETRO VOICE HOLDING
Hot Stock in Momentum play for week

OTC: PHVC
This company is nasdaq bound

Petro Voice in on a roll earning Contrac

This is not a Fly by Night
Real market Cap, Real Earnings

Here are some the latest news on PHVC:
```

Fig. Spam e-mails are a Serious Problem. These e-mails Cover a Wider Range of Topics. In Addition to Promoting Different Products, Providing Information on Stocks and Shares is Very Popular.

These advantages have not prevented the development of valuable projects such as the online user-generated encyclopaedia, Wikipedia, where strict procedures exist for the regulation of content.

However, the same technology can also be used by offenders to:

- Publish false information (e.g. about competitors);
- Libel (e.g. leaving slanderous or libellous messages);
- Disclose secret information (e.g. the publication of State secrets or sensitive business information).

It is vital to highlight the increased danger presented by false or misleading information. Defamation can seriously injure the reputation and dignity of victims to a considerable degree, as online statements are accessible to a worldwide audience. The moment information is published over the Internet, the author(s) often loses control of this information. Even if the information is corrected or deleted shortly after publication, it may already have been duplicated (“mirroring”) and made available by people that are unwilling to rescind or remove it.

In this case, information may still be available in the Internet, even if it has been removed or corrected by the original source. Examples include cases of ‘runaway e-mails’, where millions of people can receive salacious, misleading or false e-mails about people or organisations, where the damage to reputations may never be restored, regardless of the truth or otherwise of the original e-mail. Therefore the freedom of speech and protection of the potential victims of libel needs to be well balanced.

Spam and Related Threats

“Spam” describes the emission of unsolicited bulk messages.

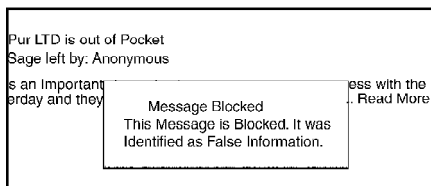


Fig. Internet Forums where Anybody can Leave Messages without Formally Registering are Popular Places to Leave Messages Containing False Information.

Although various scams exist, the most common one is e-mail spam. Offenders send out millions of e-mails to users, often containing advertisements for products and services, but frequently also malicious software. Since the first spam e-mail was sent in 1978, the tide of spam e-mails has increased dramatically.

Today, e-mail provider organisations report that as many as 85 to 90 per cent of all e-mails are spam. The main sources of spam e-mails in 2007 were: the United States (19.6 per cent of the recorded total); People's Republic of China (8.4 per cent); and the Republic of Korea (6.5 per cent). Most e-mail providers have reacted to rising levels of spam e-mails by installing anti-spam filter technology. This technology identifies spam using keyword filters or black-lists of spammers' IP addresses. Although filter technology continues to develop, spammers find ways around these systems - for example, by avoiding keywords. Spammers have found many ways to describe "Viagra", one of the most popular products offered in spam, without using the brand-name.

Success in the detection of spam e-mails depends on changes in the way spam is distributed. Instead of sending messages from a single mail server (which is technically easier for e-mail providers to identify, due to the limited number of sources), many offenders use botnets to distribute unsolicited e-mails. By using botnets based on thousands of computer systems, each computer might send out only a few hundred e-mails. This makes it more difficult for e-mail providers to identify spam by analysing the information about senders and more difficult for law enforcement agencies to track offenders. Spam e-mails are highly profitable as the cost of sending out billions of e-mails is low – and even lower, where botnets are involved. Some experts suggest the only real solution in the fight against spam is to raise transmission costs for senders. A report published in 2007 analysed the costs and profits of spam e-mails. Based on the results of the analysis, the cost of sending out 20 million e-mails is around USD 500. Since costs for offenders are low, sending spam is highly profitable, especially

if offenders are able to send billions of e-mails. A Dutch spammer reported a profit of around USD 50,000 by sending out at least 9 billion spam emails. In 2005, the OECD published a report analysing the impact of spam on developing countries. Developing countries often express the view that Internet users in their countries suffer more from the impact of spam and Internet abuse. Spam is a serious issue in developing countries, where bandwidth and Internet access are scarcer and more expensive than in industrialised countries. Spam consumes valuable time and resources in countries where Internet resources are rarer and more costly.

Other Forms of Illegal Content

The Internet is not only used for direct attacks, but also as a forum for:

- Soliciting, offers and incitement to commit crimes;
- Unlawful sale of products;
- Provision of information and instructions for illegal acts (e.g. how to build explosives).

Many countries have put in place regulations on the trade of certain products. Different countries apply different national regulations and trade restrictions to various products such as military equipment. A similar situation exists for medicines - medicines which are available without restriction in some countries may need prescription in others. Cross-border trade may make it difficult to ensure that access to certain products is restricted within a territory. Given the popularity of the Internet, this problem has grown.

Web-shops operating in countries with no restrictions can sell products to customers in other countries with restrictions, undermining these limitations. Prior to the Internet, it was difficult for most people to access instructions on how to build weapons. The necessary information was available (e.g. in books dealing with chemical aspects of explosives), but timeconsuming to find. Today, information on how to build explosives is available over the Internet and ease of access to information increases the likelihood of attacks.

OFFENCES

One of the vital functions of the Internet is the dissemination of information. Companies use the Internet to distribute information about their products and services. In terms of piracy, successful companies may face problems on the Internet comparable to those that exist outside the network. Their brand image and corporate design may be used for the marketing of counterfeit products, with counterfeiters copying logos as well as products and trying to register the domain related to that particular company. Companies that distribute products directly over the Internet can face legal problems with copyright violations. Their products may be downloaded, copied and distributed.

Copyright Related Offences

With the switch from analogue to digital, digitalisation has enabled the entertainment industry to add additional features and services to movies on DVD, including languages, subtitles, trailers and bonus material. CDs and DVDs have proved more sustainable than records and video-tapes. Digitalisation has opened the door to new copyright violations. The basis for current copyright violations is fast and accurate reproduction. Before digitalisation, copying a record or a video-tape always resulted in a degree of loss of quality. Today, it is possible to duplicate digital sources without loss of quality, and also, as a result, to make copies from any copy.

The most common copyright violations include:

- Exchange of copyright-protected songs, files and software in file-sharing systems;
- The circumvention of Digital Rights Management systems.

File-sharing systems are peer-to-peer -based network services that enable users to share files, often with millions of other users. After installing file-sharing software, users can select files to share and use software to search for other files made available by others for download from hundreds of

sources. Before file-sharing systems were developed, people copied records and tapes and exchanged them, but file-sharing systems permit the exchange of copies by many more users. Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks.

The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of French Internet users have downloaded music or files in filesharing systems, with other OECD countries showing similar trends. File-sharing systems can be used to exchange any kind of computer data, including music, movies and software. Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more and more important.

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network. Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users. The decentralised concept of secondgeneration file-sharing networks makes it more difficult to prevent them from operating.

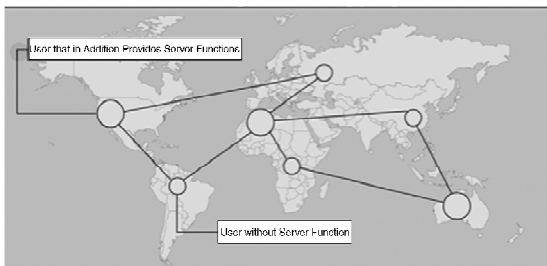


Fig. The Graphic Shows the Functioning of Second-generation File-sharing Systems. First-generation File-sharing Systems were based on Centralised Servers Hosting Lists of Available Documents. In Second –generation File-sharing Systems, the Server Function is Delegated to Users, Making it more Difficult to take down the Network and Prevent Copyright Violations.

However, due to direct communications, it is possible to trace users of a network by their IP-address. Law enforcement agencies have had some success investigating copyright violations in file-sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult.

File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses. Not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorised copies or artwork within the public domain. Nevertheless, the use of file-sharing systems poses challenges for the entertainment industry. It is unclear to what extent falls in sales of CD/DVDs and cinema tickets are due to the exchange of titles in file-sharing systems.

Research has identified millions of file-sharing users and billions of downloaded files. Copies of movies have appeared in file-sharing systems before they were officially released in cinemas at the cost of copyright-holders. The recent development of anonymous file-sharing systems will make the work of copyrightholders more difficult, as well as law enforcement agencies. The entertainment industry has responded by implementing technology designed to prevent users from making copies of CDs and DVDs such as Content Scrambling Systems (CSS), an encryption technology preventing content on DVDs from being copied.

This technology is a vital element of new business models seeking to assign access rights to users more precisely. Digital Rights Management (DRM) describes the implementation of technologies allowing copyright-holders to restrict the use of digital media, where customers buy limited rights only (*e.g.*, the right to play a song during one party). DRM offers the possibility of implementing new business models that reflect copyright-holders' and users' interests more accurately and could reverse declines in profits. One of the biggest difficulties with these technologies is that copyright protection technology

can be circumvented. Offenders have developed software tools that enable the users to make copy-protected files available over the Internet free of charge or at low prices. Once DRM protection is removed from a file, copies can be made and played without limitation.

Efforts to protect content are not limited to songs and films. Some TV stations (especially Pay-TV channels) encrypt programmes to ensure that only paying customers can receive the programme. Although protection technologies are advanced, offenders have succeeded in falsifying the hardware used as access control or have broken the encryption using software tools.

Without software tools, regular users are less able to commit offences. Discussions on the criminalisation of copyright violations not only focus on file-sharing systems and the circumvention of technical protection, but also on the production, sale and possession of “illegal devices” or tools that are designed to enable the users to carry out copyright violations.

Trademark Related Offences

Trademark violations are similar to copyright violations, a well-known aspect of global trade. Violations related to trademarks have transferred to cyberspace, with varying degrees of criminalisation under different national penal codes.

The most serious offences include:

- The use of trademarks in criminal activities with the aim of misleading targets;
- Domain or name-related offences.

The good reputation of a company is often linked directly with its trademarks. Offenders use brand names and trademarks fraudulently in a number of activities, including phishing, where millions of e-mails are sent out to Internet users resembling e-mails from legitimate companies *e.g.*, including trademarks.

Cybercrime: An Introduction

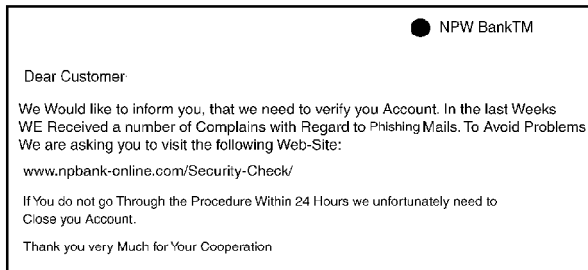


Fig. The Figure Shows a Phishing-mail. Phishing Mails are Designed to Resemble Communications from Legitimate Companies. Offenders Often Use Original Trademark-protected Logos.

Another issue related to trademark violations is domain-related offences such as cyber-squatting, which describes the illegal process of registering a domain name identical or similar to a trademark of a product or a company. In most cases, offenders seek to sell the domain for a high price to the company or to use it to sell products or services misleading users through their supposed connection to the trademark. Another example of a domain-related offence is “domain hijacking” or the registration of domain names that have accidentally lapsed.

COMPUTER RELATED OFFENCES

This category covers a number of offences that need a computer system to be committed.

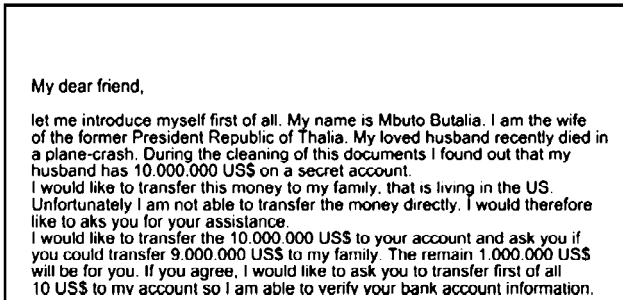
Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles, including:

- Computer-related fraud;
- Computer-related forgery, phishing and identity theft;
- Misuse of devices.

Fraud and Computer Related Fraud

Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals’ identities. Automation enables offenders to make large profits from a number of small

acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a 'small' loss, victims are less likely to invest time and energy in reporting and investigating such crimes. One example of such a scam is the Nigeria Advanced Fee Fraud.



My dear friend,

let me introduce myself first of all. My name is Mbuto Butalia. I am the wife of the former President Republic of Thalia. My loved husband recently died in a plane-crash. During the cleaning of this documents I found out that my husband has 10.000.000 US\$ on a secret account. I would like to transfer this money to my family. that is living in the US. Unfortunately I am not able to transfer the money directly. I would therefore like to aks you for your assistance. I would like to transfer the 10.000.000 US\$ to your account and ask you if you could transfer 9.000.000 US\$ to my family. The remain 1.000.000 US\$ will be for you. If you agree, I would like to ask you to transfer first of all 10 US\$ to mv account so I am able to verify your bank account information.

Fig. The Graphic Shows a Classic e-mail Based on the Advance Fee Fraud Scam. In Order to Receive the Supposed Profit, Recipients are Asked to Transfer a Certain Amount in Advance. It is a Very Popular Fraud-scam but due to the Missing Manipulation of a Computer System it is not a Computer-related fraud.

Although these offences are carried out using computer technology, most criminal law systems categorise them not as computer-related offences, but as regular fraud. The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognised as fraud. Where offenders target computer or data-processing systems, offences are often categorised as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes.

Online Auction Fraud

Online auctions are now one of the most popular e-commerce services. In 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace. Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices. Offenders committing

crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers. The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cyber crimes.

The two most common scams include:

1. Offering non-existent goods for sale and requesting buyers to pay prior to delivery;
2. Buying goods and asking for delivery, without intention to pay.

In response, auction providers have developed protection systems such as the feedback/comments system. After each transaction, buyer and sellers leave feedback for use by other users as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first. However, criminals have responded and circumvented this protection through using accounts from third parties. In this scam called "account takeover", offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

Advance Fee Fraud

In Advanced Fee Fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts. The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly.

Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent

e-mails. Current researches show, that despite various information campaigns and initiatives advance fee frauds are still growing – with regard to the number of victims as well as with regard to the total losses.

Computer Related Forgery

Computer related forgery describes the manipulation of digital documents - for example, by:

- Creating a document that appears to originate from a reliable institution;
- Manipulating electronic images (for example, pictures used as evidence in court);
- Altering text documents.

The falsification of e-mails includes the scam of “phishing” which is a serious challenge for law enforcement agencies worldwide. “Phishing” seeks to make targets disclose personal/secret information. Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target. The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails. The e-mail asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers, etc.

In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use *e.g.*, by legislation recognising digital signatures.

**with the hope, that the term will be ex-
them to transfer a rather small amount.**

Fig. Compared to the Falsification of Classic Documents, Electronic Data can Rather Easily be Manipulated. Technical Solutions Such as Digital Signatures can Prevent Unrecognised Manipulations.

Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated. For forensic experts, it is difficult to prove digital manipulations, unless technical protection is used to protect a document from being falsified.

Identity Theft

The term identity theft—that is neither consistently defined nor consistently used—describes the criminal act of fraudulently obtaining and using another person’s identity. These acts can be carried out without the help of technical means as well as online by using Internet technology.

In general the offence described as identity theft contains three different phases:

1. In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.
2. The second phase is characterised by interaction with identity-related information prior to the use of those information within criminal offences. An example is the sale of identity-related information. Credit card records are for example sold for up to 60 US dollars.
3. The third phase is the use of the identity-related information in relation with a criminal offence. In most cases the access to identity-related data enables the perpetrator to commit further crimes. The perpetrators are therefore not focusing on the set of data itself but the ability to use them in criminal activities. Examples for such offence can be the falsification of identification documents or credit card fraud.

The methods used to obtain data in phase one cover a wide range of acts. The offender can use physical methods and for example steal computer storage devices with identity-related data, searching trash (“dumpster diving”) or mail theft.

In addition they can use search engines to find identity-related data. "Googlehacking" or "Googledorks" are terms that describe the use of complex search engine queries to filter through large amounts of search results for information related to computer security issues as well as person information that can be used in identity theft scams. One aim of the perpetrator can for example be to search for insecure password protection systems in order to obtain data from this system. Reports highlight the risks that can go along with the legal use of search engines for illegal purposes.

Similar problems are reported with regard to file-sharing systems. The United States Congress discussed recently the possibilities of file-sharing systems to obtain personal information that can be abused for identity theft. Apart from that the offenders can make use of insiders, who have access to stored identity-related information, to obtain that information. The 2007 CSI Computer Crime and Security Survey shows that more than 35 per cent of the respondents attribute a percentage of their organization's losses greater than 20 per cent to insiders. Finally the perpetrators can use social engineering techniques to persuade the victim to disclose personal information. In recent years perpetrators developed effective scams to obtain secret information (e.g. bank account information and credit card data) by manipulating users through social engineering techniques.

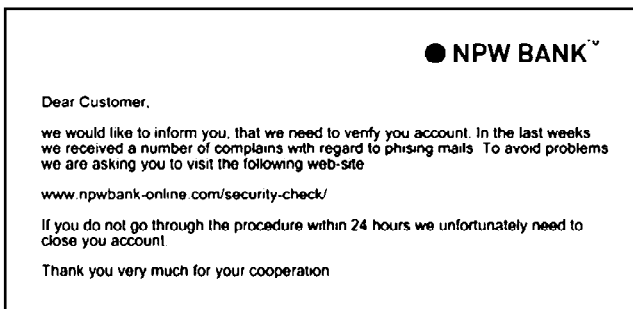


Fig. Phishing Mails are Used to Obtain Secret Information (Such as Account Information, Password and Transaction Numbers) from Targets. This Information can be used by Offenders to Commit Offences.

The type of data the perpetrators target varies. The most relevant data are:

- *Social security number (SSN) or passport number:* The SSN that is for example used in the United States is a classical example of a single identity-related data that perpetrators are aiming for. Although the SSN was created to keep an accurate record of earnings it is currently widely used for identification purposes. The perpetrators can use the SSN as well as obtained passport information to open financial accounts, to take over existing financial accounts, establish credit or run up debt.
- *Date of birth, address and phone numbers:* Such data can in general only be used to commit identity theft if they are combined with other pieces of information (e.g. the SSN). Having access to additional information like the date of birth and the address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently on a large scale available in the Internet – either published voluntarily in one of the various identity-related fora or based on legal requirements as imprint on websites.
- *Password for non-financial accounts:* Having access to passwords for accounts allows perpetrators to change the settings of the account and use it for their own purposes. They can for example take over an e-mail account and use it to send out mails with illegal content or take over the account of a user of an auction platform and use the account to sell stolen goods.
- *Password for financial accounts:* Like the SSN information regarding financial accounts is a popular target for identity theft. This includes checking and saving accounts, credit cards, debit cards, and financial planning information. Such information is an important source for an identity thief to commit financial cyber crimes.

Identity theft is a serious and growing problem. Recent figures show that, in the first half of 2004, 3 per cent of United States households fell victim to identity theft. In the United Kingdom, the cost of identity theft to the British economy was calculated at 1.3 billion British pounds every year.

Estimates of losses caused by identity theft in Australia vary from less than 1 billion USD to more than 3 billion USD per year. The 2006 Identity Fraud Survey estimates the losses in the United States at 56.6 billion USD in 2005. Losses may be not only financial, but may also include damage to reputations. In reality, many victims do not report such crimes, while financial institutions often do not wish to publicise customers' bad experiences.

The actual incidence of identity theft is likely to far exceed the number of reported losses. Identity theft is based on the fact that there are few instruments to verify the identity of users over the Internet. It is easier to identify individuals in the real world, but most forms of online identification are more complicated. Sophisticated identification tools (*e.g.*, using biometric information) are costly and not widely used. There are few limits on online activities, making identity theft easy and profitable.

Misuse of Devices

Cyber crime can be committed using only fairly basic equipment. Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.

The tools needed to commit complex offences are widely available over the Internet, often without charge. More sophisticated tools cost several thousand dollars. Using these software tools, offenders can attack other computer systems at the press of a button.

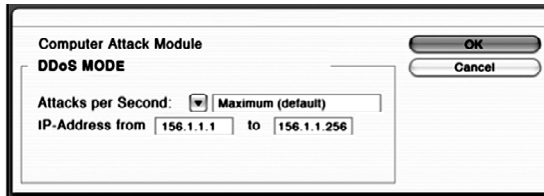


Fig. A Number of Tools are Available that Enable Offenders to Automate attacks against all Computer Systems Using IP-addresses Within a Predefined IP Range. With the Help of Such Software, it is Possible to Attack Hundreds of Computer Systems within a few Hours.

Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets.

Software tools exist to:

- Carry out DoS attacks;
- Design computer viruses;
- Decrypt encrypted communication;
- Illegally access computer systems.

A second generation of software tools has now automated many cyber-scams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less experienced computer users to commit cyber crime. Spam-toolkits are available that enable virtually anybody to send out spam emails. Software tools are now available that can be used to up- and download files from file-sharing systems. With greater availability of specially-designed software tools, the number of potential offenders has risen dramatically. Different national and international legislative initiatives are being undertaken to address cyberscam software tools—for example, by criminalising their production, sale or possession.

COMBINATION OFFENCES

There are a number of terms used to describe complex scams covering a number of different offences.

Examples include:

- Cyber terrorism;
- Cyberlaundering;
- Phishing.

Cyber terrorism

Back in the 1990s the discussion about the use of the network by terrorist organisations was focussing on network-based attacks against critical infrastructure such as transportation and energy supply (“Cyber terrorism”) and the use of information technology in armed conflicts (“cyberwarfare”).

The success of virus and botnet attacks has clearly demonstrated weaknesses in network security. Successful Internet-based attacks by terrorist are possible, but it is difficult to assess the significance of threats and at that time the degree of interconnection was small compared to the current status and it is very likely that this – apart from the interest of the states to keep successful attacks confidential – is one of the main reasons why very few such incidents were reported. At least in the past, falling trees therefore posed a greater risk for energy supply than successful hacking attacks.

This situation changed after the 9/11 attacks. An intensive discussion about the use of ICTs by terrorists started. This discussion was facilitated by reports that the offenders used the Internet within the preparation of the attack. Although the attacks were not cyber-attacks, as the group that carried out the 9/11 attack did not carry out an Internet-based attack, the Internet played a role within the preparation of the offence. Within this context, different ways in which terrorist organisations use the Internet were discovered.

Today it is known that terrorists use ICTs and the Internet for:

- Propaganda;
- Information gathering;
- Preparation of real-world attacks;
- Publication of training material;
- Communication;

- Terrorist financing;
- Attacks against critical infrastructures.

This shift in the focus of the discussion had a positive effect on research related to cyber terrorism as it highlighted areas of terrorist activities that were rather unknown before. But despite the importance of a comprehensive approach, the threat of Internet-related attacks against critical infrastructure should not move out of the focus of the discussion. The vulnerability of and the growing reliance on information technology makes it necessary to include Internet-related attacks against critical infrastructure in strategies to prevent and fight cyber terrorism.

But despite the more intensive research the fight against Cyber terrorism remains difficult. A comparison of the different national approaches shows many similarities in the strategies. One of the reasons for this development is the fact that the international communities recognised that the threats of international terrorism require global solutions. But it is currently uncertain if this approach is successful or if the different legal systems and different cultural backgrounds require different solutions.

An evaluation of this issue carries unique challenges because apart from reports about major incidents there are very few data available that could be used for scientific analysis. The same difficulties arise with regard to the determination of the level of threat related to the use of information technology by terrorist organisations. This information is very often classified and therefore only available to the intelligence sector. Not even a consensus of the term "terrorism" was yet achieved. A CRS Report for the United States Congress for example states that the fact that one terrorist booked a flight ticket to the United States via the Internet is proof that terrorists used the Internet in preparation of their attacks. This seems to be a vague argumentation as the booking of a flight ticket does not become a terrorist-related activity just because it is carried out by a terrorist.

In 1998 only 12 out of the 30 foreign terrorist organisations that are listed by the United States State Department, maintained websites to inform the public about their activities. In 2004 the United States Institute of Peace reported that nearly all terrorist organisations maintain websites – among them Hamas, Hezbollah, PKK and Al Qaida. Terrorists have also started to use video communities (such as YouTube) to distribute video messages and propaganda. The use of websites and other forums are signs of a more professional public relations focus of subversive groups. Websites and other media are used to disseminate propaganda, describe and publish justifications of their activities and to recruit new and contact existing members and donors. Websites have been used recently to distribute videos of executions.

Information Gathering

Considerable information about possible targets is available over the Internet. For example, architects involved in the construction of public buildings often publish plans of buildings on their websites.

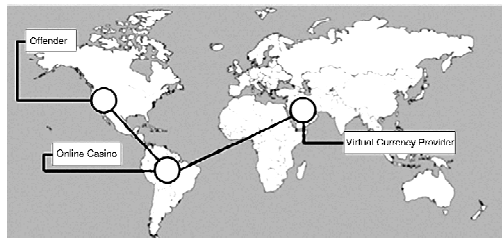


Fig. The Graphic Illustrates the Combination of Online Casinos and Virtual Currencies in Internet-based Money-laundering scams. By Using such Services, Offenders can Make it Difficult for Law Enforcement Agencies to Track Transfer Processes and Identify Offenders.

Today high resolution satellite pictures are available free of charge on various Internet services that years ago were only available to very few military institutions in the world. Furthermore, instructions on how to build bombs and even

virtual training camps that provide instructions on the use of weapons in an e-Learning approach were discovered.

In addition, sensitive or confidential information that is not adequately protected from search-robots and can be accessed via search engines. In 2003, the United States Department of Defence was informed that a training manual linked to Al Qaeda contained information that public sources could be used to find details about potential targets. In 2006 the New York Times reported that basic information related to the construction of nuclear weapons were published on a Government Web site that provided evidence about the Iraq approaches to develop nuclear weapons.

A similar incident was reported in Australia where detailed information about potential targets for terrorist attacks was available on Government websites. In 2005 the press in Germany reported that investigators found that manuals on how to build explosives were downloaded from the Internet onto the computer of two suspects that tried to attack public transportation with self-built bombs.

Preparation of Real-world Attacks

There are different ways that terrorists can make use of information technology in preparing their attack. Sending out e-mails or using forums to leave messages are examples that will be discussed in the context of communication. Currently more direct ways of online preparations are discussed.

Reports were published that point out that terrorists are using online games within the preparation of attacks. There are various different online games available that simulate the real world. The user of such games can make use of characters (avatar) to act in this virtual world. Theoretically those online games could be used to simulate attacks but it is not yet uncertain to what extent online games are already involved in that activity.

Publication of Training Material

The Internet can be used to spread training material such as instructions on how to use weapons and how to select

targets. Such material is available on a large scale from online sources. In 2008, Western secret services discovered an Internet server that provided a basis for the exchange of training material as well as communication. Different websites were reported to be operated by terrorist organisations to coordinate activities.

Communication

The use of information technology by terrorist organisations is not limited to running websites and research in databases. In the context of the investigations after the 9/11 attacks it was reported that the terrorists used e-mail communication within the coordination of their attacks. The press reported about the exchange of detailed instructions about the targets and the number of attackers via e-mail. By using encryption technology and means of anonymous communication the communication partner can further increase the difficulties in identifying and monitoring terrorist communication.

Terrorist Financing

Most terrorist organisations depend on financial resources they receive from third parties. Tracing back these financial transactions has become one of the major approaches in the fight against terrorism after the 9/11 attacks. One of the main difficulties in this respect is the fact that the financial resources required to carry out attacks are not necessary high.

There are several ways in which Internet services can be used for terrorist financing. Terrorist organisations can make use of electronic payment systems to enable online donations. They can use websites to publish information how to donate, e.g., which bank account should be used for transactions. An example of such an approach is the organisation "Hizb al-Tahrir" which published bank account information for potential donators. Another approach is the implementation of online credit card donations. The Irish Republican Army (IRA) was one of the first terrorist organisations that offered donations via credit card.

Both approaches carry the risk that the published information will be discovered and used to trace back financial transactions. It is therefore likely that anonymous electronic payment systems will become more popular. To avoid discovery terrorist organisations are trying to hide their activities by involving nonsuspicious players such as charity organisations. Another (Internet-related) approach is the operation of fake web-shops.

It is relatively simple to set up an online-shop in the Internet. One of the biggest advantages of the network is the fact that businesses can be operated worldwide. Proving that financial transactions that took place on those sites are not regular purchases but donations is quite difficult. It would be necessary to investigate every transaction – which can be difficult if the online shop is operated in a different jurisdiction or anonymous payment systems were used.

Attacks against Critical Infrastructures

In addition to regular computer crimes such as fraud and identity-theft, attacks against critical information infrastructures could become a target for terrorists. The growing reliance on information technology makes critical infrastructure more vulnerable to attacks.

This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks. In those cases the disruption caused by a network-based attack goes beyond the failure of a single system. Even short interruptions to services could cause huge financial damages to e-Commerce businesses – not only for civil services but also for military infrastructure and services. Investigating or even preventing those attacks presents unique challenges. Unlike physical attacks, the offenders do not need to be present at the place where the effect of the attack occurs. And while carrying out the attack the offenders can use the means of anonymous communication and encryption technology to hide their identity. Investigating such attacks requires special procedural instruments, investigation

technology and trained personnel. Critical infrastructure is widely recognised as a potential target of a terrorist attack as it is by definition vital for a state's sustainability and stability. An infrastructure is considered to be critical if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state. These are in particular: electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina in the United States highlights the dependence of society on the availability of those services.

The vulnerabilities of critical infrastructure with regard to network-based attacks can be demonstrated by highlighting some of incidences related to air-transportation.

- The check-in systems of most airports in the world are already based on interconnected computer systems. In 2004 the Sasser computer worm infected million of computers around the world, among them computer systems of major airlines, which forced the cancellation of flights.
- Today a significant number of tickets are purchased online. Airlines use information technology for various operations. All major airlines allow their customers to buy tickets online. Like other e-commerce activities, those online services can be targeted by offenders. One common technique used to attack web-based services is Denial-of- Service (DoS) attacks. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, Ebay and Amazon. As a result, some of the services were not available for several hours or even days. Airlines have been affected by DoS attacks as well. In 2001 the Lufthansa Web site was the target of an attack.
- Another potential target for Internet-related attacks against critical air transportation infrastructure is the airport control system. The vulnerability of computer-controlled flight control systems was demonstrated by

a hacking attack against Worcester Airport in the U.S., in 1997. During the hacking attack, the offender disabled phone services to the airport tower and shut down the control system managing the runway lights.

Cyberwarfare

Cyberwarfare describes the use of ICTs in conducting warfare using the Internet. It shares a number of features in common with Cyber terrorism. Discussions originally focused on the substitution of classic warfare by computer-mediated or computer-based attacks. Network-based attacks are generally cheaper than traditional military operations and can be carried out even by small states. Protection against cyber attack is difficult. Until now, there have been limited reports on the substitution of armed conflicts by Internet-based attacks. Current discussions focus on attacks against critical infrastructure and control of information during a conflict.



Fig. Over Recent Years, the Internet has become an Important Medium for Information and Propaganda Exchange During Armed Conflicts. It is Often Discussed how far it is Possible and/or Advisable to Disable Certain Internet Services During Progressive key Stages of a Conflict.

In considering both civil and military communications, information infrastructure is a key target in armed conflicts. However, it is uncertain if these attacks will be carried out via the Internet. Attacks against computer systems in Estonia and the United States have been linked with cyberwarfare. Since attacks cannot be traced back to official state organisations with any certainty, it is difficult to categorise them as cyberwarfare. Attacks against infrastructure that are carried out physically – e.g. by arms and explosives—are also difficult to categorise as cyberwarfare. The control of information has always been an important issue in armed conflicts, as information can be used to influence the public, as well as

opposing military personnel. Control of information over the Internet will become an increasingly important means of influence during armed conflicts.

Cyberlaundering

The Internet is transforming money-laundering. With larger amounts, traditional money-laundering techniques still offer a number of advantages, but the Internet offers several advantages. Online financial services offer the option of enacting multiple, worldwide financial transactions very quickly. The Internet has helped overcome the dependence on physical monetary transactions. Wire transfers replaced the transport of hard cash as the original first step in suppressing physical dependence on money, but stricter regulations to detect suspicious wire transfers have forced offenders to develop new techniques. The detection of suspicious transactions in the fight against money-laundering is based on obligations of the financial institutions involved in the transfer.

Money-laundering is generally divided into three phases:

1. Placement;
2. Layering;
3. Integration.

With regards to the placement of large amounts of cash, the use of the Internet might perhaps not offer that many tangible advantages. However, the Internet is especially useful for offenders in the layering (or masking) phase. In this context the investigation of money-laundering is especially difficult when money-launderers use online casinos for layering. The regulation of money transfers is currently limited and the Internet offers offenders the possibility of cheap and tax-free money transfers across borders. Current difficulties in the investigation of Internet-based money-laundering techniques often derive from the use of virtual currencies and the use of online casinos.

The Use of Virtual Currencies

One of the key drivers in the development of virtual currencies were micro-payments, where the use of credit cards

is problematic. With the growing demand for micro-payments, virtual currencies, including 'virtual gold currencies', were developed. Virtual gold currencies are account-based payment systems where the value is backed by gold deposits. Users can open e-gold accounts online, often without registration. Some providers even enable direct peer-to-peer (person-to-person) transfer or cash withdrawals. Offenders can open e-gold accounts in different countries and combine them, complicating the use of financial instruments for money-laundering and terrorist financing. Accountholders may also use inaccurate information during registration to mask their identity.

The Use of Online Casinos

Unlike a real casino, large financial investments are not needed to establish online casinos. In addition, the regulations on online and offline casinos often differ between countries. Tracing money transfers and proving that funds are not prize winnings, but have instead been laundered, is only possible if casinos keep records and provide them to law enforcement agencies.

Current legal regulation of Internet-based financial services is not as stringent as traditional financial regulation. Apart from gaps in legislation, difficulties in regulation arise from:

- *Difficulties in customer verification:* accurate verification may be compromised, if the financial service provider and customer never meet.
- *Due to lack of personal contact:* it is difficult to apply traditional know-your-customer procedures; and
- Internet transfers often involve the cross-border participation of providers in various countries.
- The lack of law/penal code for monitoring certain instruments is particularly difficult when providers allow customers to transfer value in a peer-to-peer model.

Phishing

Offenders have developed techniques to obtain personal information from users, ranging from spyware to "phishing"

attacks. "Phishing" describes acts that are carried out to make victims disclose personal/secret information. There are different types of phishing attacks, but e-mail-based phishing attacks contain three major phases. In the first phase, offenders identify legitimate companies offering online services and communicating electronically with customers whom they can target *e.g.*, financial institutions. Offenders design websites resembling the legitimate websites ("spoofing sites") requiring victims to perform normal log-in procedures, enabling offenders to obtain personal information (*e.g.* account numbers and online banking passwords). In order to direct users to spoofing sites, offenders send out e-mails resembling e-mails from the legitimate company, often resulting in trademark violations.

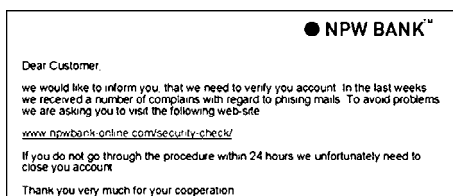


Fig. A Phishing E-mails are Designed to Look Like an E-mail from a Legitimate Company in Order to make the Victim Disclose Secret Information. Very Often the Offenders are Targeting for Customers of Financial Institutions.

The false e-mails ask recipients to log-in for updates or security checks, or by threats (*e.g.* to close the account) if users do not cooperate. The false e-mail generally contains a link that victim should follow to the spoof site, to avoid users manually entering the correct web address of the legitimate bank.

Offenders have developed advanced techniques to prevent users from realising that they are not on the genuine Web site. As soon as personal information is disclosed, offenders log in to victims' accounts and commit offences such as the transfer of money, application for passports or new accounts, etc., The rising number of successful attacks proves phishing's potential. More than 55,000 unique phishing sites were reported to the APWG in April 2007. Phishing techniques are

not limited to accessing passwords for online banking only. Offenders may also seek access codes to computers, auction platforms and social security numbers, which are particularly important in the United States and can give rise to “identity theft” offences.

ECONOMIC IMPACT OF CYBER CRIME

Without any doubt, the financial damage caused by computer and Internet crimes is significant. Various recent surveys have been published analysing the economic impact of cyber crime, highlighting its significant impact. The same general concerns about crime statistics also apply to estimates of financial damage – it is uncertain to what extent surveys provide accurate figures and statistics, as many victims may not report crimes.

Results of Selected Surveys

The Computer Security Institute (CSI) Computer Crime and Security Survey 2007 analysed the economic impact of cyber crime, based on the responses of 494 computer security practitioners in U.S corporations, government agencies and financial institutions. It is mainly relevant for the United States. Taking into account the economic cycle, the survey suggests that, after rising until 2002, the financial impact of cyber crime decreased over the following years.

The survey suggests that this finding is controversial, but it is unclear why the number of reported crimes and the average loss of the victims may have decreased. In 2006, the extent of losses climbed again. The survey does not explain the reduced losses in 2002 or the rise in 2006. From 21 categories identified by the survey, the highest dollar losses were associated with financial fraud, viruses, system penetration by outsiders and theft of confidential data. The total losses for 2006 of all respondents amounted to some USD 66.9 million. After a number of years of decreasing average losses per respondent, a turnaround is taking place. In 2006, the average loss was USD 345,000. In 2001, the average loss was nearly ten times higher (USD 3.1 million). The average

loss per respondent depends strongly on the composition of respondents - if mainly small and medium sized enterprises (SMEs) respond one year and are replaced by larger companies the next year, the change in participants strongly affects the statistical results.

The FBI Computer Crime Survey 2005 follows an approach similar to the CSI Survey, but with a greater and more extensive coverage. The FBI survey estimates that the cost of security incidents from computer and Internet crimes amounted to USD 21.7 million. The most popular offences that detected by respondents organisations were virus attacks, spyware, port scans and sabotage of data or networks. The FBI Computer Crimes Survey 2005 includes an estimate of the total loss for the United States economy.

Based on average losses and the assumption that some 20 per cent of US organisations are affected by computer crime, a total loss of USD 67 billion was calculated. However, there are concerns as to how representative these estimates are, and the consistency of participants year on year. The 2007 Computer Economics Malware Report focuses on the impact of malware on the worldwide economy by summing up total estimated costs caused by attacks. One of its key findings is the fact that offenders designing malicious software are shifting from vandalism to a focus on financial profits.

The report finds that the financial losses caused by malware attacks peaked in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion), but have reduced Since, 2004 to USD 13.3 billion in 2006. However, similar to the survey results, there is uncertainty as to whether the statistics on the impact of malware are realistic.

There are large discrepancies between reported losses and proven damages – take the case of the Sasser Worm, for example. Millions of computer systems were reported to be infected. In the civil law suit against the software designer, very few companies and private individuals responded to the request to prove their losses and join the lawsuit. The case ended with a settlement that the designer of the virus should pay compensation of less than ten thousand US dollars.

It is unclear how representative the statistics on the economic impact of cyber crime are and whether they provide reliable information on the extent of losses. It is uncertain to what extent cyber crime is reported, not only in surveys, but also to law enforcement agencies. Authorities engaged in the fight against cyber crime encourage victims of cyber crime to report these crimes.

Access to more precise information about the true incidence of cyber crimes would enable law enforcement agencies to better prosecute offenders, deter potential attacks and enact more appropriate and effective legislation. Several public and private sector organizations have tried to quantify the direct and indirect costs of malware. While it is difficult to estimate the cost to businesses, it is even more difficult to assess the financial losses inflicted by malware and the like to individual consumers, although there is scattered evidence that damages can be very large.

However, such costs have different components. They may result in direct damages to hardware and software as well as financial and other damages due to identity theft or other fraudulent schemes. The range of estimates differs, although the emerging overall picture is quite coherent. Businesses on the other hand may avoid reporting cyber crime offences for several reasons: Businesses may fear that negative publicity could damage their reputation.

If a company announces that hackers have accessed their server, customers may lose faith. The full costs and consequences could be greater than the losses caused by the hacking attack. However, if offenders are not reported and prosecuted, they may go on to reoffend. Targets may not believe that law enforcement agencies will be able to identify offenders. Comparing the large number of cyber crimes with the few successful investigations, targets may see little point in reporting offences. Automation also means that cybercriminals follow a strategy of reaping large profits from many attacks targeting small amounts (*e.g.*, as happens with

advance fee fraud). For only small amounts, victims may prefer not to go through with time-consuming reporting procedures. Reported cases are often based on extremely high fees. By targeting only small amounts, offenders design scams that will often not be followed up.

Chapter 3

Global Threat of Economic and Cyber Crime

GROWTH OF ECONOMIC CRIME

Economic Crime Defined

The lack of agreed upon definitions regarding economic crime and computer crime, has resulted in a paucity of data and information on the size and scope of the problem. There are no national mechanisms, such as the Uniform Crime Reports, for the reporting of economic crimes by law enforcement. Academics have not been able to agree on definitions and have for the most part continued to focus on white-collar crime. White-collar crimes require that the perpetrator be a person of status who has opportunity because of his position in an organization. This definition, while seminal in the 1940's, is inaccurate today and impedes agreement on more contemporary definitions.

Based on Sutherland's limited definition, all other crimes are viewed as newer versions of conventional crimes. Thus, the true nature of the amount of economic crime is buried in the statistics of more conventional crimes.

For example, credit card fraud is typically classified as a larceny instead of access device fraud. In 1995 the National Fraud Investigation Center undertook the task of creating a classification system that would be able to categorise and classify fraud information in a dynamic and hierarchical structure. The Fraud Identification Codes (FIC) were designed hierarchically to allow classification of each type of fraud in order of importance, and thus, provide the ability to add and

modify types as it became necessary. Four levels of classification were developed, from the most general to the more specific: Class, Sub-class, Type and Sub-type. The following groups reviewed and recommended changes to the FIC: The Uniform Crime Reporting Division of the FBI, The National Incident Based Reporting System of the FBI, The White Collar Crime Division of the FBI, the American Bankers Association Check Fraud Unit, and the Secret Service.

The FIC system currently has over 600 classified types of fraud including 11 classes, 75 subclasses, over 350 types and over 175 sub-types. Without a framework and a single reporting center, economic crime statistics will continue to be fragmented estimates of the true extent of the level of the crimes.

A system such as the FIC codes could provide the logical format for a national Programme to gather data on economic crimes. In order to address the issue of economic crime in the United States, it is necessary to adopt a definition for the purpose of this white paper.

The definition as suggested, follow is:

- Economic Crime is defined as an illegal act (or a constantly evolving set of acts) generally committed by deception or misrepresentation (fraud) by someone (or a group) who has special professional or technical skills for the purposes of personal or organizational financial gain or to gain (or attempt to gain) an unfair advantage over another individual or entity.

This definition provides for the inclusion of more contemporary crimes and methods in situations where the individual is not a person of status in an organization or even employed by the organization. It does not refer to these types of crimes as non-violent, as most definitions of white-collar crimes do.

Increasingly, organised crime groups have used economic crime to fuel their enterprises, such as arms trafficking, drug smuggling, and terrorism, and have used violence to further their ends.

Statutory Law

There seems to be no limit to the types of economic crimes and the methods of committing them. However, certain crimes are unique to certain industries. For example, cloning applies to the wireless telecommunication industry and currency transaction reporting applies primarily to the banking and financial services industry. The discussion that follows relates to specific economic crimes in nine different areas and the laws enacted by Congress that proscribe the illegal conduct.

Mail and Wire Fraud: Generic Frauds and Swindles

The mail fraud statute was enacted in 1872. The law was designed specifically to enable special agents of the U.S. Mail to investigate frauds and swindles perpetrated through the use of the mail system and to seek federal prosecution for such offenses. Because it applies to “any scheme or artifice to defraud, or for obtaining money or property by false pretenses, representations or promises,” the statute has been used to prosecute fraudulent insurance claims, fraudulent loan applications, securities frauds, and an unlimited variety of frauds and swindles.

It frequently is applied to new types of fraudulent acts in those situations where Congress has not had the opportunity to enact a specific statute to deal with the crime. Because mail fraud has generic appeal, it applies to conventional economic crimes in the eight areas on which this report focuses. The crime of mail fraud is committed by depositing or receiving matter with or from the Postal Service or a private interstate carrier or causing matter to be delivered by the Postal Service or such carrier for the purpose of furthering the fraudulent scheme.

There is no monetary threshold necessary for prosecution, although federal prosecutors informally may decline to handle minor cases. The wire fraud statute is patterned after the mail fraud statute. It proscribes the use of interstate

communications by wire, radio or television to perpetrate a scheme or artifice to defraud. The statute is generic in application and applies to a wide range of criminal activity across industries.

Courts have not limited the reach of the statute to land line telephone communications; the statute has been applied to wireless communications using microwave technology, in part. Because transactions over the Internet usually involve interstate communications by telephone wire or cable, the wire fraud statute will continue to serve as an effective law enforcement and prosecutorial tool to combat cyber crimes against all major industries.

Banking Industry: Financial Institution Crimes

Like mail and wire fraud, the bank fraud statute applies generically to any scheme to defraud a financial institution or any fraudulent act designed to obtain money or property from a financial institution. The statute currently defines a financial institution as any depository institution insured by the FDIC, as well as credit unions and the Federal Reserve Bank. Unlike mail or wire fraud, which are limited to the medium of communication, the bank fraud statute applies to any fraudulent scheme designed to obtain money or property from the financial institution, including check forging, check kiting, stolen checks, credit card fraud, fraudulent loan applications, student loan fraud, and embezzlement.

The financial statement statute applies to any fraudulent statement made to a financial institution for the purpose of obtaining money or property in the custody or control of the institution. The quintessential financial statement fraud is a false statement made in an application for a loan or to obtain credit from a financial institution.

The Continuing Financial Crimes Enterprise (CFCE) statute was enacted in 1990 and is designed to impose criminal sanctions for large-scale frauds committed upon financial institutions, such as the massive frauds upon the savings and loan industry. A CFCE is a series of violations of numerous sections of title 18 of the U.S. Code, as well as the crimes of

mail and wire fraud, if they affect a financial institution, committed by one who organises, manages or supervises the enterprise, and receives \$5 million in gross receipts from the enterprise over a 24-month period. It is limited to financial institutions as victims, but would include a series of credit card frauds, if those crimes were charged under 18 U.S.C. § 1341, 1343 or 1344.

The computer fraud statute currently prohibits accessing a “protected computer” without authority, or in excess of authority, to obtain information or to obtain something of value, hacking into a protected computer and transmitting a Programme, information, code, or command with the intent to damage the computer, or transmitting in interstate commerce any threat to cause damage to a protected computer in order to extort something of value. Because a “protected computer” includes a computer “exclusively for the use of a financial institution” or if not exclusively used, a computer “used by or for a financial institution and the conduct constituting the Offence affects that use by or for the financial institution”, the statute applies to specific criminal conduct directed at bank computers or computerised data storage facilities. The money laundering statutes were enacted in 1986 as part of the Money Laundering Control Act.

These sections apply to the conduct of the customer of a financial institution who deposits the proceeds of criminal activity with the bank and uses the bank to layer or launder those proceeds and to facilitate the transportation of the proceeds into or out of the country. Banks providing online services and electronic wire transfers are particularly susceptible to such conduct.

In 1970, Congress enacted the Bank Secrecy Act, also known as the Currency and Foreign Transaction Reporting Act, to curb the laundering of cash through banking institutions. That Act requires the filing of currency transaction reports (CTR's) for any deposit or withdrawal of cash exceeding \$10,000. Subsequent amendments to the Act require the filing of reports for the transportation of currency or monetary instruments exceeding \$10,000 into or out of the U.S., cash

transactions exceeding \$10,000 at casinos or as part of business transactions, and for suspicious activity transactions. The Treasury Department has promulgated several regulations providing the details of the reporting requirements, which apply to both electronic fund transfers and online banking transactions.

The Racketeering Influenced and Corrupt Organizations (RICO) statute has application to mail fraud, wire fraud, bank fraud, currency transaction reporting violations and money laundering because they are predicated acts constituting racketeering activity. RICO provides an effective law enforcement weapon against those who engage in a pattern of racketeering activity and victimise a financial institution, or those financial institutions that engage in a pattern of racketeering activity.

Credit Card Crimes

In addition to mail and wire fraud, Congress has enacted two laws that specifically address the traditional means of committing crimes involving a credit card. The credit card fraud statute prohibits the sale, use or transportation of a counterfeit, altered, stolen, lost or fraudulently obtained credit card in a transaction affecting or using interstate or foreign commerce, or furnishing money obtained through the use of a counterfeit, altered, stolen, lost or fraudulently obtained card, or the receipt or concealment of goods or tickets for interstate or foreign transportation obtained through the use of such a card.

Federal courts disagree whether this crime can be committed without a plastic card. Because online transactions involve the use of the credit card number and not the card itself, it is unclear whether section 1644 applies to online transactions. The access device statute, however, defines an "access device" to include a card or an account number. This statute prohibits the production, use or trafficking in counterfeit credit cards or account numbers, the possession of 15 or more counterfeit cards or account numbers, producing, trafficking in or possessing equipment used to produce

counterfeit cards, without authority from the card issuer, offering a card or selling information regarding applications to obtain cards, or attempts or conspiracies to commit any of the acts regarding credit cards or account numbers.

Health Care Fraud

Prior to 1996, federal prosecutors employed generic crimes such as the false statements statute, false claims statute, mail fraud statute or wire fraud statute to prosecute those charged with engaging in conduct encompassed by the term "health care fraud." In some instances, prosecutors were able to use laws created to address specific methods of committing health care fraud relating to the Medicare and Medicaid Programmes, such as the false claims statute, the anti-kickback statute, and the self-referral statute.

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), which created five distinct health care fraud crimes. This enactment was significant in that it imposes criminal penalties for health care frauds perpetrated upon private health care benefit plans, as well as Medicare and Medicaid. "Health care fraud" under HIPAA is committed by executing or attempting to execute a scheme or artifice to defraud any health care benefit Programme or fraudulently obtaining the money or property of a health care benefit Programme.

HIPAA also proscribes the theft or embezzlement of funds, securities, premiums, property and other assets of a health care benefit Programme, concealment of a material fact or fraudulent statements in connection with the delivery or payment of health care benefits or services, and the obstruction of or interference with the communication of records relating to a violation of HIPAA to a criminal investigator. Additionally, a conspiracy to violate any of those offenses also is a crime. Federal financial statement fraud and false claims fraud have limited application to the health care industry because the victim in those statutes is the government. The enactment of HIPAA significantly enhances the prosecutorial arsenal available to combat health care fraud committed by traditional

means because the victim of those crimes are health care benefit Programmes, which include private health insurance plans. The Act, however, does not address a myriad of other cyber crimes that are health care related, for example, pharmaceutical fraud, web sites that fraudulently purport to provide medical advice, and phony web sites. The only statutory tool currently available to prosecute such conduct effectively is the wire fraud statute.

Insurance Fraud

Most fraudulent conduct impacting upon the insurance industry constitutes application fraud or claims fraud. These frauds may be committed by the insured, an agent or employee of the company, a third party, or as is more often the case, a conspiracy between two or more of those groups.

Historically, insurance fraud has been the subject of state regulation. Nevertheless, federal jurisdiction and laws may be invoked where the fraudulent activity constitutes a mail or wire fraud, which is frequently the case. Applications for insurance are commonly sent through the mail or processed online over the Internet. Proofs of loss, bills, invoices and receipts submitted in support of an insurance claim typically are transmitted to the insurer by mail or by fax transmission. Further, a continuing pattern of such activity may constitute a RICO crime. Federal law also regulates the conduct of persons or entities engaged in the business of insurance.

It imposes criminal sanctions for:

- The embezzlement or misappropriation of premiums, money or other property of insurance companies,
- The making of false statements or reports to an insurance regulatory agency or official involving the overvaluing of land, property or security for the purpose of influencing action by that agency,
- Making false entries in any book, report or statement of the insurance company to deceive the company or an insurance agency or official regarding the financial solvency of the business,
- Engaging in the insurance business by any person

convicted of a felony involving dishonesty or a breach of trust,

- Threatening, influencing or obstructing the administration of law in any pending proceeding before an insurance regulatory agency or official.

There is no published decision to date regarding prosecutions under this section. Section 1034 authorises the U.S. Attorney General to seek civil penalties or injunctions for violations of section 1033.

Securities Fraud

Congress created numerous securities fraud crimes by enactment of the Securities and Exchange Act of 1934. The major anti-fraud statute is section 10(b) of the Act, which is codified at 15 U.S.C. § 78j (b). That section and Rule 10b-5, which was promulgated by the Securities Exchange Commission, prohibit the use of any instrumentality of interstate commerce or stock exchange or mail for the commission of a fraudulent act, scheme or artifice to defraud, or the making of a false statement in connection with the purchase or sale of a security. Although that statute and rule have served as an effective prosecutorial weapon in combating securities fraud and insider trading, the statute was not drawn with the Internet and e-trading in mind.

Telecommunication Fraud

Fraud impacts all sectors of the communications industry—telephone, wireless, and cable. The types of fraud are numerous: toll fraud, including “clip-on” and “shoulder surfing” methods, call-sell operations established by organised crime groups who engage “phreaks” to hack into phone line, subscription fraud, which frequently also involves identity theft, PBX fraud, which also involves call-sell operations, calling card fraud, remote call forwarding, and computer terrorism/sabotage.

Because these frauds frequently encompass interstate wire communications, the wire fraud statute is an effective legal weapon to combat telecommunication fraud. The principal

fraudulent activities impacting upon the wireless communication industry are subscription fraud and cloning. Subscription fraud occurs when an individual applies for and obtains a wireless telephone account.

Because a fraudulent application customarily involves the use of a counterfeit or stolen credit card or account number, or a stolen means of identification, the credit card fraud, access device fraud, and identity fraud statutes are available for the prosecution of such Behaviour. Most wireless service providers currently encourage customers to apply by accessing their web site. The wire fraud statute serves as an additional prosecutorial weapon to combat online subscription fraud. Cloning entails the theft of an electronic serial number (ESN) and mobile identification number (MIN) assigned to a legitimate wireless phone, and the installation of those numbers on a stolen phone. Once accomplished, the cloned stolen phone behaves like the phone owned by the legitimate customer, and the monthly bill for charges are sent to the legitimate customer.

The access device statute specifically proscribes the theft of ESNs and MINs, the production or use of a cloned phone, and the possession, use, production or trafficking in scanning receivers or hardware or software utilised to clone phones for the purpose of obtaining unauthorised wireless services. Although cloning a phone and the use of a cloned phone historically has not involved the Internet, technology is now in place to enable wireless access to the Internet. The access device statute should continue to be an effective legal weapon to combat the use of cloned phones for Internet access.

Additionally, the computer fraud statute may also apply to such conduct. Congress initially sought to regulate abuses committed by the telemarketing industry by enactment of the Telephone Consumer Protection Act of 1991. That Act provides for statutory damages for each violation, but does not impose criminal sanctions. In 1994, Congress enacted the Senior Citizens Against Marketing Scams (SCAMS) Act. The SCAMS Act imposes criminal penalties for telemarketing frauds involving wire communications, including conspiracies to commit such crimes, and enhanced sentences where senior

citizens are victimised. Because Internet scams encompass the use of wire communications in part, the wire fraud statute will remain an effective legal weapon for the prosecution of scammers.

Intellectual Property and Computer Crime

The computer fraud statute seeks to address conduct involving the use of computers to perpetrate the crime and computers as the victims of crime.

The statute imposes criminal penalties for:

- Accessing a computer without authorization to obtain classified federal information to be used for the benefit of a foreign nation.
- Accessing a computer without authorization to obtain the financial record of a financial institution, issuer of a credit card, consumer reporting agency or federal agency.
- Accessing a government computer without authorization and affecting the government's use of the computer.
- Accessing a protected computer (a "protected computer" is a computer either used in interstate or foreign commerce or exclusively for the use of a financial institution or the U.S. government) without authorization and with the intent to defraud and obtaining anything of value through that fraudulent act.
- Transmitting a Programme, information, code or command and intentionally causing damage to a protected computer.
- Accessing a protected computer and causing damage.
- Trafficking in any password that can be used to access a computer if the trafficking affects interstate or foreign commerce, or "such computer is used by or for the Government of the United States."
- Transmitting any threat to cause damage to a protected computer in order to extort money or other thing of value.

To the extent that credit card account numbers constitute computer data on various e-commerce web sites, accessing the computers or peripheral equipment for the purposes of unlawfully obtaining and trafficking in stolen account numbers may also constitute computer fraud. A recent example of such conduct is the hacker identified as Maxim who attempted to extort \$100,000 from CD Universe and, when the threat failed, posted credit card account numbers that he had obtained from CD Universe's web site on another web site.

Because the use of a modem involves a wire communication, the wire fraud statute applies to the use of a computer to commit crimes, including credit card transactions, online banking, online insurance fraud, etc. Prior to 1996, the principal federal weapon designed to combat the theft of trade secrets was the Trade Secrets Act.

That statute prohibits the unauthorised disclosure of confidential information by government employees. Prosecutions for trade secret theft that victimised the private sector were based on the National Stolen Property Act, which was not particularly effective because it did not encompass intangibles (soft property) within its protective embrace, or the mail or wire fraud statute. The Economic Espionage Act of 1996 attempted to cure previous deficiencies by imposing criminal penalties for economic espionage by or for foreign government and for the theft of trade secrets from public and private sector sources. Moreover, the 1996 statute defines the theft of trade secrets to include a misappropriation committed by any means, as well as the receipt of trade secrets. The Trademark Counterfeiting Act of 1984 imposes criminal penalties for the intentional trafficking in counterfeit goods and services, *i.e.*, those goods and services that bear a stolen trademark. Congress first imposed criminal sanctions for copyright infringements in 1897. Since that time, the statute has been amended on numerous occasions as Congress attempted to provide more protection to the copyright holder. Notably in 1992, the Copyright Felony Act added protection against large-scale computer software piracy, and in 1997

Congress enacted the No Electronic Theft Act, which removed the requirement that the perpetrator derive a financial gain from the infringement.

Identity Theft

The federal identity fraud statute prohibits the unlawful production, possession, transfer or use of a “means of identification” of another person to commit or abet any federal crime or state felony crime or to defraud the federal government. The statute defines a “means of identification” as any name or number used to identify an individual, including an access device.

Because access devices include a credit card account number, the crime of identity fraud encompasses the use of another person’s credit card account number, as opposed to use of the plastic card itself. The statute also includes other devices as “means of identification,” including a passport, birth certificate, driver’s license, social security number, taxpayer identification number, unique electronic identification number, and unique biometric data, such as a fingerprint, voice print, retina or iris image. By 1999, twenty states had enacted identity theft statutes. Many other states prosecute identity theft under criminal impersonation statutes. The success of identity theft prosecutions under those impersonation statutes depends upon the language of each statute.

IMPACT OF TECHNOLOGY ON ECONOMIC CRIME

The growth of the information age and the globalization of Internet communication and commerce have impacted significantly upon the manner in which economic crimes are committed, the frequency with which those crimes are committed, and the difficulty in apprehending the perpetrators. A recent survey conducted by the Gartner Group of 160 retail companies selling products over the Internet reveals that the amount of credit card fraud is twelve times higher online than in the physical retail world. There is no reason to believe that this figure is unique to the credit card industry. Another recent study indicates that the number of search warrants issued by

the federal government for online data has increased 800 per cent over the past few years. Technology has contributed to that increase in four major respects—anonymity, security (or insecurity), privacy (or the lack of it) and globalization. Additionally, technology has provided the medium or opportunity for the commission of traditional crimes.

Criminals continue to make false statements in credit applications submitted over the Internet, bank employees continue to embezzle funds by wire transfer or account takeover, and swindlers continue to misrepresent products at auction sites over the Internet. However, it is the widespread use of technology and the Internet for business transactions and communications, and the confluence of anonymity, security, privacy and globalization that have exposed the public and private sectors to an alarming new array of cyber attacks. In addition to their inability to prevent such attacks, both government and the private sector lack effective enforcement tools and remedies to bring the perpetrators to justice. Technology and the Internet have contributed to the growth of economic crime in each of the identified industries in similar ways.

Anonymity enables the criminal to submit fraudulent online applications for bank loans, credit card accounts, insurance coverage, brokerage accounts, and health care coverage or to construct a counterfeit web site in order to establish an inflated value for publicly traded stock in order to sell the stock at a falsely inflated price (“pump and dump” schemes). Anonymity also enables employees to pilfer corporate assets. For example, bank employees can embezzle money through electronic fund transfers and employees of credit card issuers can capture account numbers and sell them to outsiders, electronically transferring the account numbers to the conspirators.

Further, anonymity provides enhanced opportunities for two types of perpetrators—the organised crime mobster and the teenage hacker. Security, or the lack of it, enables criminal hackers to disrupt e-commerce in several ways. They can engage in denial of service attacks, compromise payment

systems in online banking, penetrate web sites and extract credit card account numbers for resale or as ransom for the extortion of cash from the card issuer, or hijack a web site for the purpose of stealing the identity of the e-commerce merchant, directing the proceeds of sales to the hijacker. Privacy protections enable thieves to take advantage of the benefits of anonymity, while hampering the efforts of law enforcement and private sector fraud investigators to track the thieves. Lastly, the Internet enables communication and commerce to occur beyond or without borders, presenting significant problems in the prevention, investigation and enforcement of those crimes.

Banking

There is no pending legislation that specifically addresses frauds in connection with online banking. The Internet provides fertile ground for those intending to defraud financial institutions. Because the online customer is anonymous, the risk of fraud is greater. Projected increases in the volume of online transactions and repeal of the Glass-Steagall Act, which has expanded the types of institutions that may provide banking services, could increase the exposure to cyber attack. Congressional focus is currently on cyber laundering, specifically the electronic transfer of funds into U.S. banks from sources outside the country and subsequent transfers by those banks to cyber laundering havens. On the regulatory side, the Federal Trade Commission and other agencies have proposed regulations dealing with the privacy of financial data, the circumstances when disclosure may be made, and the conditions precedent to such disclosures.

Those regulations, which are scheduled to take effect on November 13, 2000, require financial institutions to provide privacy notices to consumers, limit the disclosure of nonpublic personal information to nonaffiliated third parties, and allow consumers to opt-out of certain restrictions. The Electronic Signature in Global and National Commerce Act, which became law on July 1, 2000, is a major effort to facilitate the consummation of contracts, including agreements with banking

and financial institutions, electronically. While the Act facilitates e-Commerce, it provides yet another opportunity for the theft of a significant aspect of one's identity—the signature. The Act contains no provision imposing criminal sanctions for the theft or piracy of one's signature. The access device statute should be amended to include electronic and digital signatures as a “means of identification. Additional legislation is essential to reduce the risks presented by anonymity and database insecurity, including prescribed authentication procedures and encryption protections.

Credit Card

The use of credit cards for online retail purchases, as well as for online gambling and to gain access to pornography and child pornography sites, is expected to increase exponentially. Online transactions are not conducted face-to-face; therefore, the merchant cannot identify the customer in the traditional manner. The increased volume of online transactions and the absence of face-to-face interaction provide greater opportunity for fraud, including identity theft for the purpose of conducting an online transaction.

While substantive laws provide ample redress for the criminal use of credit cards (and debit cards) in cyberspace, the implementation of new technologies for credit purchases, such as smart cards and electronic wallets, may raise issues regarding the applicability of existing criminal statutes. Those statutes should be amended to prohibit the theft or fraudulent sale, distribution or possession of a counterfeit, stolen or fictitious account number regardless of whether that account number is used in connection with a plastic card, electronic wallet or other form of digital storage.

The amendment should also state that the crime applies to the theft by computer of account numbers or information that could be used to identify an account number. There is currently no pending legislation that would regulate the use of credit cards for online transactions. However, S. 699, the Telemarketing Fraud and Seniors Protection Act, would amend the wire fraud statute to include schemes or artifices to defraud,

perpetrated via Internet communications. Because credit card fraud can be prosecuted under this statute, the proposed legislation would enhance significantly the enforcement arsenal for credit card fraud. Further, the proposed Identity Theft Protection Act of 2000 would strengthen protection against fraudulent practices committed with stolen credit cards.

That Act requires the card issuer to confirm any reported change of address and notify the cardholder of any request for additional cards. It also requires credit-reporting agencies to inform the card issuer if the address on the application for a credit card is different than the address shown in the consumer's records. Section 4 of the Act would also add a requirement that, upon the request of the consumer, a consumer reporting agency must include a fraud alert in the consumer's file and notify each person seeking credit information of the existence of that alert. That Act would provide significant protection from the technological identity theft.

Health Care

Currently, there is no pending legislation designed to address health care frauds committed in cyberspace. Future legislative attention should focus on the attributes of the Internet and e-commerce that promote fraudulent activity in the provision of health care products and services.

Insurance

There currently are no pending federal laws or regulations that address insurance fraud committed in cyberspace. Historically, regulation of the insurance business has been the province of the states. The 1999 Gramm- Leach-Bliley Act, which repealed the Glass-Steagall Act, enabled financial institutions to provide a variety of services, including insurance. The federal government should establish broad legislation designed to regulate and secure the online sale of insurance products.

Arguably, the only effective weapon at the disposal of federal prosecutors is the wire fraud statute. Additional

legislation that requires secure connections and seeks to prevent fraudulent activity regarding online insurance applications and claims should be a priority.

Moreover, because the Internet is an instrument of interstate commerce, Congress should rethink that portion of the Gramm-Leach-Bliley Act which leaves the regulation of issues such as the use of nonpublic information by insurance companies to the state regulators. Federal involvement in this area would provide uniform regulation and would not subject financial institutions that provide banking, securities and insurance products to a different regulatory scheme for the offering of insurance products.

Securities

The Internet is an instrument of interstate commerce. Thus, section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 provide criminal sanctions for fraudulent acts committed in cyberspace involving the purchase or sale of securities. Also, the mail fraud and wire fraud statutes provide an additional weapon for the prosecution of frauds and swindles involving securities.

Again, substantive criminal laws provide ample sanction for fraudulent conduct impacting upon the securities industry. The Securities Exchange Commission is, however, faced with the difficult task of detecting and investigating securities frauds committed in the online venue. It has created a new enforcement unit to deal specifically with online trading and frauds committed with respect to securities, but legislation is required to assist investigators in the detection and investigation of such frauds. The Online Investor Protection Act of 1999, S. 1015, would be a start in that direction.

Telecommunications

Section 699, The Telemarketing Fraud and Senior Protection Act would amend the wire fraud statute to prohibit fraudulent telemarketing practices over the Internet. That statute should be further amended to prohibit fraudulent conduct over the Internet transacted in part through a wireless connection.

Although existing criminal laws will continue to provide effective weapons to combat cyber crimes committed upon the traditional service industries that offer their services and products through e-commerce, Congress and the global community must move swiftly to provide an effective array of substantive laws designed specifically for Internet transactions. That array should include laws and treaties to provide law enforcement and the private sector with the tools essential for the detection and investigation of cyber crime.

Some Congressional attention has focused on peripheral issues such as privacy and encryption, and there are signs that Congress is beginning to address Internet-specific issues. Five pending Congressional bills suggest that Congress is aware that law enforcement must be equipped with adequate resources and remedies to combat cyber crime. A High Tech Crime Bill was introduced on February 24, 2000 by senators Charles Schumer and John Kyl.

This bill proposes amendments to the computer fraud statute that would include fraudulent acts committed upon "protected computers" in the United States, by persons in foreign countries and would include damage done to computers and computer systems irrespective of property damage losses. That amendment would encompass damage caused by, for example, denial of service attacks.

The proposed bill also would amend 18 U.S.C. § 3123 (c), enabling law enforcement to employ trap and trace devices to assist in the investigation of computer attacks. The Internet Security Act of 2000, introduced in April 2000 by Senator Leahy, would expand the jurisdictional scope of the computer fraud statute to include international hacking. It would amend section 3123 to enable law enforcement to employ trap and trace devices, impose encryption standards, and authorize the prosecution of juvenile hackers. It would also appropriate \$25 million for each of the next four fiscal years for law enforcement training Programmes in computer fraud investigations. Both bills seek to react to recent attacks upon

e-Commerce sites, including the denial of service attacks. The Internet Integrity and Critical Infrastructure Protection Act of 2000, introduced on April 13, 2000 by Senator Hatch, co-sponsored by Senator Schumer, would impose criminal penalties for cyber hacking committed by persons under 18 years old, create a National Cyber Crime Technical Support Center to serve as a resource center for federal, state and local law enforcement and assist them in the investigation of computer-related crimes, and provide the implementation of computer crime mutual assistance agreements in order to enable reciprocal assistance for foreign authorities.

Also on April 13, 2000, Senator Hutchinson introduced S. 2451 that would increase the criminal penalties for computer fraud committed in violation of 18 U.S.C. § 1030 and establish a National Commission on Cyber security to study incidents of computer crimes and the need for enhanced methods of combating such crimes. Finally, on May 9, 2000, Congressman Boehlert introduced the Law Enforcement Science and Technology Act of 2000, co-sponsored by Congressman Stupak. This bill would establish an Office of Science and Technology in the Office of Justice Programmes of the Department of Justice.

The mission of that office would be:

- To serve as the national focal point for work on law enforcement technology;
- To carry out Programmes to improve the safety and effectiveness of, and access to, technology to assist Federal, State and local law enforcement agencies.

The bill would direct the appropriation of \$40 million for regional National Law Enforcement and Corrections Technology Centers, \$60 million for research and development of forensic technologies and methods to improve crime laboratories, and \$20 million for the testing and evaluation of technologies. Additional governmental attention must be focused on extradition and mutual assistance treaties that will enable the United States to prosecute cyber crimes committed by international terrorists and hackers.

Consumers

Very few studies on fraud victimization have been conducted. Two that studied telemarketing are Harris and Associates and a study by the American Association of Retired Persons. The most comprehensive study to date is the National White Collar Crime Center's National Public Survey on White Collar Crime. The study's goal was, "to present a picture of what the average American thinks about white collar crime."

Its survey of 1,169 households throughout the United States found that:

- Over 1 out of 3 households had been victimised by white collar crime in the last year.
- Widely held opinions concerning the profile of typical white collar crime victims are divorced from the actual profile of victims found by recent research on victimization.
- There is a disparity between how Americans believe they will react if victimised and how they do react when they are actually victimised.
- Less than 1 in 10 victimizations were ever reported to law enforcement or consumer protection agencies.
- The public has a deep concern with increasing the apprehension and sanctioning of white collar criminals.

Consumer victimization usually results in three types of losses: privacy, good credit status, and funds or assets. Consumers are concerned that personal information disclosed to companies with which they do business may be compromised.

Such compromises include unauthorised access and/or by the company's employees, lack of security to protect the information, providing the information to third parties, and the maintenance of accurate information. Any one of these breaches could result in the consumer's personal information falling into criminal hands, which could easily result in identity

theft. Other consequences range from damage to an individual's credit rating to the loss of funds and/or assets.

Industry

The victimization of industry falls into four categories:

1. Profit losses
2. Damage to reputation
3. Loss of continuity of business
4. Loss of intellectual property

According to The Credit Risk Management Report, "The average organization loses more than \$9 a day per employee to fraud and abuse. The average organization loses about 6 percent of its total annual revenue to fraud and abuse committed by its own employees. Fraud and abuse costs US organizations more than \$400 billion annually."

Early on, many corporations were able to take the position that fraud was a cost of doing business, and could make it up by passing the cost of fraud to the consumer through increased prices. In more competitive markets this is not possible. In those cases when the bottom line is hit hard by fraud, executives are less reluctant to commit funds to fraud management and computer security.

While big business can sustain a major loss to fraud, many small businesses have suffered severely and in some cases have gone out of business as a result of their fraud losses. This often occurs because these small organizations cannot afford sophisticated hardware and software to prevent and detect fraud. Because corporations are afraid that reporting fraud may damage their reputation, they are reluctant to do so.

They fear legal retaliation if they share or disclose too much, and are afraid that their consumers and stockholders will lose confidence in them. The actual amount of corporate victimization is not known, because of the unwillingness of corporations to report or admit that fraud has affected them. Many e-Businesses are concerned about the continuity of their business. That is, they do not want their services to customers to be disrupted. Although security remains a significant

concern for business, consumers are paramount in e-Commerce; they want to shop quickly with no hassles. Recent distributed denial of service attacks on web sites such as e-bay and Amazon.com point to the vulnerabilities of e-Commerce. The lack of security and the intrusion of criminals (fraudulent element) both impede the growth of e-Commerce.

Intellectual property theft – in the form of trademark infringement, cyber squatters, typo squatters, trade-secret theft, and copyright infringement – has increased as Internet use and misuse has risen. It occurs across the seven industries detailed here, as well as most other businesses. “According to the American Society for Industrial Security, American businesses have been losing \$250 billion a year from intellectual property theft since the mid-1990’s.”

Government

Government suffers from several forms of victimization, much like corporations do, including theft of intellectual property, theft of assets, and loss of reputation. Several cases have been in the news where United States secrets have been compromised or potentially compromised.

These events have tarnished the reputation of several government agencies by pointing out the lack of, or loose, security procedures. Numerous federal governmental web sites have been defaced by hackers, including the CIA, FBI, and the United States Department of Justice.

Several reports of intrusions have occurred with government computers. In many of these cases, systems have been penetrated, but no classified information was accessed. Fraud, waste, abuse, and mismanagement are generally reported together.

While it is hard to get a handle on their size and scope, the Senate Governmental Affairs Committee, chaired by Senator Fred Thompson (R-Tennessee) reported on January 26, 2000, that “In 1998 alone, \$35 billion in taxpayer dollars was lost due to government waste, fraud, abuse, and mismanagement.”

Law Enforcement

On the federal level, numerous regulatory and law enforcement agencies are authorised to combat specific economic crimes, including the Federal Bureau of Investigation (FBI), United States Secret Service (USSS), the United States Postal Inspection Service, Securities and Exchange Commission (SEC), and United States Customs.

Each of these agencies has jurisdiction over the following economic crimes/fraud.

- *FBI:* health care, financial institution, intellectual property, telemarketing, securities/commodities, bankruptcy, insurance, computer, and Internet
- *Secret Service:* credit card, cellular, and computer
- *Postal Inspector:* mail and consumer
- *Securities and Exchange Commission:* insider and online trading, stock manipulation, and fraudulent stock offerings
- *United States Customs:* money laundering, cyber crimes, including child pornography and the importing of dangerous substances

On the international level, Interpol recently announced its intention to become active in the investigation of international computer crimes. Interpol announced on June 30, 2000 that it is establishing an international intelligence network to inform the public and private sectors of impending cyber attacks and potential targets for malicious hacks.

The intelligence information will be relayed to Interpol by Atomic Tangerine, a venture consulting firm, using technology (Net Radar) developed by SRI International, the parent company of Atomic Tangerine. Local law enforcement capabilities for combating economic crime vary depending on the size and location of the department, and the allocation of resources. Some larger municipalities and state law enforcement agencies have formed economic and computer crime units. As resources, training, and awareness of the

intensity of the problem increase, it is likely that more of these units will be formed.

National Fraud Center

The National Fraud Center (NFC) is an internationally recognised leader in global customised fraud and risk management solutions. Formed in 1982, its original mission was to combat insurance fraud, which, at that time, was becoming a societal concern. Since then the NFC has earned a reputation for combining expert knowledge and technology to produce solutions to fraud problems for vertical industries and the government. "Technological solutions developed with NFC's expertise have saved clients tens of millions of dollars." The NFC has an in-depth understanding of how economic crime affects businesses, consumers, and government agencies, as its researchers collect and analyse fraud data continuously.

Economic Crime Investigation Institute

The Economic Crime Investigation Institute (ECII) was formed in 1988 by Dr. Gary R. Gordon, then Director of the Economic Crime Investigation Programme at Utica College of Syracuse University, and Mr. John Martin, Esq., then Chief of Internal Security for the United States Department of Justice. Part of the Institute's mission is to support education and research in the areas of economic crime and computer security, by advising Utica College faculty on formal academic Programmes for pre-professional students and professionals in the field of economic crime investigation.

Its other goal is to develop the ECII into the premier educationally focused institute, providing a national forum that brings together all interested parties to develop solutions to economic crime problems faced by society. The ECII strives to provide a forum for individuals in government, corporate America, and higher education to discuss current economic crime issues and to promote the dissemination of information on economic crime and its investigations. The Economic Crime Investigation Institute's annual conferences are its primary way of accomplishing this.

A non-profit organization that receives federal grant funding from the Bureau of Justice Assistance, Department of Justice, the National White Collar Crime Center (NW3C) "provides a nationwide support network for enforcement agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime." Founded in 1980, the Center's focus is to support state and local agencies, using their needs as a guide for the projects and endeavors the NW3C undertakes.

In addition to its state-of-the-art financial and computer crime training course development and delivery, new projects include the development of the National Fraud Complaint Management Center (NFCMC) to leverage technology in the management of economic crime complaints and to bring added value to the prevention, investigation, and prosecution efforts surrounding complaints. A significant part of this project is the establishment of the Internet Fraud Complaint Center (IFCC) in partnership with the Federal Bureau of Investigation. The IFCC represents a unique approach to the growing problem of fraud on the Internet. The NW3C has also been selected to serve as the Operations Center for the National Cyber crime Training Partnership (NCTP), an initiative of the United States Attorney General, headed by the Computer Crimes and Intellectual Property Section of the Justice Department.

The National Coalition for the Prevention of Economic Crime

A non-profit organization established in 1996, the National Coalition for the Prevention of Economic Crime (NCPEC) provides support services to businesses in their fight against economic crime. Its mission is to reduce incidents of economic crime through cooperative, information-sharing efforts. Current training Programmes include instruction on fraud management, operational and strategic fraud management techniques, financial investigations practical skills, basic data

recovery and analysis and instruction on how to use the Internet as an investigative tool. Hosted in partnership with the NW3C, the NCPEC has established an annual national conference entitled the Economic Crime Summit which brings together academics, government, private corporations, victims' interest groups, prevention specialists, and others to examine methodologies and share ideas to address economic crime on all levels.

Internet Fraud Council

The Internet Fraud Council, a division of the National Coalition for the Prevention of Economic Crime, is composed of organizations from around the world that are interested in the prevention, investigation, and prosecution of Internet fraud. The Internet Fraud Council's mission is to provide research, education, best practices, and tools for the prevention of economic crime committed using the Internet.

Internet Fraud Complaint Center

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IFCC's mission is to address fraud committed over the Internet. For victims of Internet fraud, IFCC provides a convenient and easy way to alert authorities of a suspected criminal or civil violation. For law enforcement and regulatory agencies, IFCC offers a central repository for complaints related to Internet fraud. The data from this source can then be analysed to identify and quantify fraud patterns, as well as statistics on the current fraud trends.

The IFCC's ultimate goal is to reduce Internet fraud victimization. As stated on its web site, "Long term benefits of this Programme will be substantial. Not only will its efforts reduce the amount of economic loss by Internet fraud throughout the United States, it will enable state and local law enforcement professionals to develop and successfully prosecute criminal Internet fraud cases. IFCC will also serve

as the catalyst that allows law enforcement and regulatory authorities to network and share fraud data.”

Independent Corporations and Private Sector Industry Coalitions

As a result of limited law enforcement resources, corporations on their own or in cooperation with industry coalitions, such as BITS, the technology group for the Financial Services Roundtable, have had to initiate strategic economic crime management plans and investigative groups. There is a growing level of frustration among these corporations, because the monetary thresholds for law enforcement even to investigate a case, let alone prosecute, can be very high, depending on the jurisdiction.

Coupled with this, is increased legislation requiring corporations to institute anti-fraud Programmes and compliance departments. While the protection of corporate assets and their consumers should be their responsibility, there are several consequences to this arrangement. Many economic crimes go unreported, fewer prosecutions of these offenses occur, and perpetrators tend to be fired rather than prosecuted, leaving them free to move on to another organization and continue their victimization.

FUTURE NEEDS AND CHALLENGES

Law Enforcement Training

Specialised training in the areas of economic and computer crime, and how they affect specific industries, as well as computer forensics, needs to continue to increase for law enforcement personnel. Without an understanding of how specific industries function, it is difficult to investigate or prosecute economic crimes.

New career paths within law enforcement organizations could be established before promotions and reassignments drain agencies of their limited skilled personnel in technically sophisticated areas. Often, individuals develop expertise and then are promoted or reassigned, making it necessary to train

new people from ground zero. Unless the individuals who have expertise, experience, and contacts in industry are given an incentive to stay in their units, this cycle will continue and the investigation and prosecution of economic crime will not increase or improve.

Laws, Regulations and Reporting Systems

In the United States, government (federal, state and local), with limited exceptions, has allowed self-regulation of the Internet. Government regulation has, for the most part, focused on cyber crimes that are not economic crimes, such as child pornography and cyber stalking.

Fortunately, that attitude appears to be changing. There are numerous bills pending in Congress that address criminal frauds committed on the Internet, identity theft, and issues involving Internet security and attacks upon web sites. This legislation should use language that will be easily adaptable to future technological changes to help deter future economic crimes. However, there are other gaps in legislation. There are many regulations that require businesses to protect themselves by working to prevent fraud (i.e. know your customer). However, the government sends conflicting signals when it will not assist in prevention efforts by cleaning up regulations and enacting new supporting laws, as well as providing prosecutorial support. Current government regulations covering certain industries prohibit companies from sharing information with each other. This eliminates the possibility of an instrument, such as a central database of fraud, which companies could use in their procedures for preventing and detecting fraud. It is important that legislation addressing this be written and passed. Other legislation is also necessary, such as laws that keep pace with the changing nature of credit card payment and online payment systems.

Public-Private Partnerships

No one group will be able to solve the complex problem posed by economic crime. Coalitions of private and public groups need to work together to combat economic and cyber

crime. As more of these alliances develop, there will be more resources available to reverse the trend of economic crime. College and universities need to revamp their existing Programmes, e.g. criminal justice, accounting, computer science, or create new ones to meet the changing needs of society in this area.

At this time there are only two undergraduate Programmes and one graduate Programme addressing these issues – the Economic Crime Investigations Programmes at Utica College (Utica, NY) and Hilbert College (Hamburg, NY) and the Economic Crime Management Master's Programme at Utica College. These Programmes are supported by advisory boards consisting of individuals at the top of their fields from the credit card, banking, insurance, and telecommunications industries, as well as representatives from government agencies, such as the U.S. Secret Service and the FBI. Further Congress, through the Identity Theft Assumption and Deterrence Act requires the FTC and industry to work together. Presidential Directive 63 required industry and government to work together in combating Internet/e-commerce fraud.

Balancing Privacy Interests

The growth of e-commerce and the creation of new law enforcement techniques to combat cyber crime raise critical issues concerning consumer, business and governmental privacy. The protection of individual privacy, while considered almost sacred, in the world of economic and cyber crime can actually work to the criminal's advantage. The new FBI tool, Carnivore, is an attempt to gather intelligence information, without compromising privacy.

According to the FBI's web site,

- In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet service providers (ISP) lack the ability to discriminate communications to identify a particular subject's messages to the exclusion of all

others, the FBI designed a diagnostic tool, called Carnivore.

- The Carnivore device provides the FBI with a “surgical” ability to intercept and collect the communications which are subject of the lawful order while ignoring those communications which they are not authorised to intercept.
- This is a matter of employing new technology to lawfully obtain important information, while providing enhanced privacy protection.

Carnivore provides law enforcement with the ability to keep pace with the technical advances in communication. However, this tool raises “Big Brother” concerns for the public. The controversy that Carnivore has evoked in its infancy points to the issue of trust that government, industry, and society as a whole need to resolve. BITS, Financial Services Roundtable adopted privacy principles in late 1997 that are guidelines for banking industry self-regulation concerning privacy. Industry, in general, sees self-regulation as preferable to government rule.

The BITS policy includes guidelines in each of these areas.

- Recognition of a customer’s expectation of privacy
- Use, collection, and retention of customer Information
- Maintenance of accurate information
- Limiting employee access to information
- Protection of information via established security procedures
- Restrictions on the disclosure of account information
- Maintaining customer privacy in business relationships with third parties
- Disclosure of privacy principles to customers

Several other industry organizations are developing similar guidelines. Their aim is to have self-regulation rather than government intervention. By informing customers of privacy policies, industry is attempting to engender their trust. There is a delicate balance between protecting one’s privacy, legitimate business use of personal data, and fraud prevention. However, the use of personal data for fraud prevention

and interdiction is beneficial to society. Therefore, fraud and risk management exceptions should be built into any and all laws, regulations, and policies.

In fact, the use of personal data for identity theft prevention directly reduces the number of identity theft victims. Further, many industries (*i.e.* insurance, banking and securities) require fraud prevention through regulation to protect consumers, customers, shareholders, and employees.

Effective authentication in an e-commerce transaction is not possible without the use of independent, personal verification data. Authentication is critical to the growth and confidence of e-commerce. Fraudsters have quickly learned to defeat our technical systems.

If they are allowed to opt out of databases, they will rapidly exploit our vulnerabilities to the financial detriment of the general public. Global cooperation is also needed in this area. The United States must take a leadership role in fostering cooperation throughout the global community in the development of uniform laws, meaningful and comparable privacy policies, effective assistance to prosecutions by foreign countries, and a sharing of information.

The U.S. already has surrendered a leadership role in the areas of privacy and information sharing. The European Union developed a comprehensive privacy directive applicable to all member nations in 1995, and the European Parliament recently refused to allow its member nations to share data and nonpublic information with the U.S. With respect to information sharing, Interpol has announced its intention to provide private industries throughout the world with intelligence information regarding the vulnerability of those industries or specific companies to cyber attacks. At this point, the global community perceives the U.S. as a reluctant partner, not a leader.

Global Interaction and Cooperation

For the past two decades, the international community has focused on the development of extradition treaties, mutual

legal assistance treaties, and sanctions to combat the proliferation of money laundering crimes on an international scale. The international focus for the next two decades must be directed Towards Internet crime and cyber crime. That focus cannot be limited to procedural remedies. Many countries lack substantive laws specifically designed to combat computer and Internet crimes.

For example, the alleged perpetrators of the "Love Bug" virus in the Philippines could not be charged with a substantive crime because no computer crime laws had been enacted in that country. The international community must maintain a more aggressive and comprehensive approach to cyber crime, including treaties that provide for uniform laws on cyber crime and cyber terrorism. That approach should be inspired and led by the United States.

On April 27, 2000, the Council of Europe released a draft version of its proposed International Convention on Cyber-Crime. In 1989 and 1995, the Council encouraged member governments to revise or adopt laws specific to the challenges of computer crime. However, a binding legal agreement is now considered necessary to harmonise computer crime laws and to step up investigations and ensure effective international cooperation. The Council hopes to adopt the Convention by September 2001.

The Convention draft requires each signatory nation to adopt legislation or other measures with respect to five categories of crimes:

1. Offenses against computer data and systems;
2. Computer-related forgery;
3. Computer-related fraud;
4. Child pornography;
5. Copyright and intellectual property offenses.

The Convention draft also contains uniform provisions for searches and seizures of computers and computer data, extradition, and mutual legal assistance procedures. The United States has participated in the negotiations preliminary to the release of the Convention draft. The Computer Crime and Intellectual Property Section (CCIPS) of the Department of

Justice assisted in the drafting process. U.S. government agencies, including the Department of Justice, plan to seek legislative support for the Convention. In addition, the Group of Eight (G8) nations have discussed economic crime and cyber crime during recent annual summits in London and Moscow. The issue again appeared on the summit agenda for the July meeting in Okinawa.

CCIPS chairs the G8 subgroup on high-tech crime. The OECD has made recommendations for industry and government to work together in order to combat money laundering. Guidelines have been established for authentication and "know your customer Programmes". Congress needs to address, both from a domestic and global perspective, current law enforcement tools that are needed for investigations and prosecutions in the digital environment.

Although Congress has enacted laws that facilitate global e-commerce, for example, the Electronic Signature in Global and National Commerce Act, it has not considered legislation focusing upon the investigation and enforcement of crimes committed in the e-commerce venue. For example, law enforcement needs judicial guidance, but preferably legislative authorization, regarding the search and seizure of computers and peripheral equipment, eavesdropping with new technological devices, and the preservation and presentation of digital evidence. Without Congressional initiative, state and federal courts will continue on a path of conflicting decisions that inhibit effective law enforcement investigations and effectively paralyse U.S. cooperation with foreign governments.

CONCLUSION: TRENDS AND OBSERVATIONS

According to the National White Collar Crime Center's National Public Survey on White Collar Crime, FBI statistics indicate that, for the period from 1988 to 1997, arrests for violent crimes decreased, but the arrest rate for crimes having to do with fraud and embezzlement increased dramatically. As is evident from this study, this trend is sure to continue, and to grow, as technology facilitates the emergence of cyber crime. As a result of the burgeoning of e-commerce, cyber

crime has become prevalent, and it will soon be difficult to differentiate among traditional economic and cyber crimes. Reporting of economic and cyber crime is problematic and grossly underestimated, as is apparent from the reluctance of corporations to report fraud losses and activity. The FBI's Uniform Crime Report should be revised to include specific economic crimes, following the Fraud Identification Codes established by the National Fraud Center.

Until such a means of reporting is implemented and the stigma of fraud victimization is removed, this problem will not be solved. Uniform and thorough reporting is necessary in the war on economic and cyber crime; resources for investigation and prosecution will naturally follow as the enormity of the problem unfolds. Preventing, detecting, investigating, and prosecuting economic crimes must become a priority, in order to lessen their impact on the economy and the public's confidence. Law enforcement, as it stands now, is in danger of slipping further behind the highly sophisticated criminals. New resources, support for existing organizations, e.g. The National Fraud Center, The National White Collar Crime Center, The Internet Fraud Council, and The Economic Crime Investigation Institute, and innovative solutions are needed to control this growing problem in America and the world.

This is not to say that the focus should be entirely on economic crime to the detriment of investigation and prosecution of violent crime. Certainly, it would not be in society's best interest to have violent crime increase, while economic crime decreases. However, it has often been questioned and argued whether the psychological and financial impact of economic crime on its victims is as great or greater in many instances as violent crime.

Rather, higher priority must be given to the provision of necessary resources and the passage of relevant legislation to counter the near-epidemic impact of economic crime on American society and the world. This can only be accomplished with the cooperation of the private, public, and international sectors. All stakeholders must be more willing to exchange

information on the effect economic and cyber crime has on them and the methods they are using to detect and prevent it. No one sector holds all the resources, tools or solutions. In fact, in many instances, industry has more resources than government, but must be motivated and authorised to partner and communicate. All parties must be willing to work together to effect change in existing laws and regulations and to promulgate new initiatives. The "victims" need to follow the lead of the "criminals" and organise themselves, so that the organised "bad guys" are not operating in a lawless environment, where culpability is at a minimum.

Chapter 4

Cyber Terrorism

WHY AND HOW INTERNATIONAL TERRORISTS USE THE INTERNET

The Internet is used as a prime recruiting tool for insurgents. Extremists use chat rooms, dedicated servers and websites, and social networking tools as propaganda machines, as a means of recruitment and organization, for training grounds, and for significant fund-raising through cyber crime. These websites and other Internet services may be run by international terrorist groups, transnational cyber crime organizations, or individual extremists. YouTube channels and Facebook pages of Taliban and Al Qaeda supporters may radicalise Western-based sympathisers, and also provide a means for communication between these “lone wolf” actors and larger organised networks of terrorists.

The decentralised nature of the Internet as a medium and the associated difficulty in responding to emerging threats can match the franchised nature of terrorist organizations and operations. It is unclear how great a role the Internet plays in coordinating the efforts of a single group or strategy. Many Arabic-language websites are said to contain coded plans for new attacks. Some reportedly give advice on how to build and operate weapons and how to pass through border checkpoints. Other news articles report that a younger generation of terrorists and extremists, such as those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by various nations’ law enforcement computer technology. Cyber crime has now surpassed

international drug trafficking as a terrorist financing enterprise. Internet Ponzi schemes, identity theft, counterfeiting, and other types of computer fraud have been shown to yield high profits under a shroud of anonymity.

According to press reports, Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud. There may be some evidence that terrorist organizations seek the ability to use the Internet itself as a weapon in an attack against critical infrastructures. Also, links between terrorist organizations and cybercriminals may show a desire to hone a resident offensive cyber capability in addition to serving as a means of procuring funds. To some observers, the term "Cyber terrorism" is inappropriate, because a widespread cyberattack may simply produce annoyances, not terror, as would a bomb, or other chemical, biological, radiological, or nuclear explosive (CBRN) weapon. However, others believe that the effects of a widespread computer network attack would be unpredictable and might cause enough economic disruption, fear, and civilian deaths to qualify as terrorism.

At least two views exist for defining the term Cyber terrorism as traditionally understood:

1. *Effects-based:* Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals other than terrorists.
2. *Intent-based:* Cyber terrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.

Propaganda, Recruitment, and Training

In a July 2005 letter to Abu Musab al-Zarqawi, the late leader of Al Qaeda operations in Iraq, senior Al Qaeda leader Ayman al-Zawahiri wrote, "We are in a battle, and more than half of this battle is taking place in the battlefield of the media."

Terrorist organizations exploit the Internet medium to raise awareness for their cause, to spread propaganda, and to inspire potential operatives across the globe. Websites operated by terrorist groups can contain graphic images of supposed successful terrorist attacks, lists and biographies of celebrated martyrs, and forums for discussing ideology and methodology. The Quetta Shura Taliban reportedly maintains several dedicated websites, including one with an Arabic-language online magazine, and publishes daily electronic press releases on other Arabic-language jihadist forums.

The As-Shahab Institute for Media Production is Al Qaeda Central's media arm and distributes audio, video, and graphics products online through jihadist forums, blogs, and file-hosting websites. A recent online English-language terrorist propaganda periodical called *Inspire* appears to have originated from the media arm of a Yemen-based Al Qaeda group and contains articles by Anwar al-Awlaki, an English-speaking, U.S.-born radical imam whose sermonizing rhetoric and calls to action make extensive use of cyberspace. Al-Awlaki has been connected to several terrorist plots, including the attempted Times Square bombing in New York City in May 2010.

Al-Awlaki has also been either directly or indirectly linked to radicalizing Nidal M. Hasan, who allegedly committed the November 2009 shooting at Fort Hood, Texas, and Umar Farouk Abdulmutallab, the Nigerian suspect accused of trying to ignite explosives on Northwest/Delta Airlines Flight 253 on Christmas Day 2009. Faisal Shahzad, a naturalised U.S. citizen from Pakistan, admitted to trying to set off a car bomb in Times Square and said he was inspired by al-Awlaki's online lectures. Some experts question the authenticity of the periodical *Inspire* and its link to Al Qaeda. The effectiveness of violent images used to reach its mainstream target audience is debated, as the violent images may appeal only to a small, self-selected segment of the population. Al-Zawahiri, in a reference to winning the "hearts and minds" of Muslims, noted that "the Muslim populace who love and support you will never find palatable... the scenes of slaughtering the hostages." These websites can also carry step-by-step instructions on how to

build and detonate weapons, including cyber weapons. One Web site reportedly carries a downloadable “e-jihad” application, through which a user can choose an Internet target and launch a low-level cyberattack, overwhelming the targeted Web site with traffic in order to deny its service.

The websites may also contain instructions for building kinetic weapons, such as bombs and improvised explosive devices, as well as for conducting surveillance and target acquisition. The Internet can also be used to transmit information and material support for planned acts of terrorism. A recent case involving a U.S. citizen residing in Pennsylvania alleges that a woman using the nickname “JihadJane” posted messages on YouTube and used jihadist websites and chat rooms to plan and facilitate an overseas attack.

Cyber Crime and Fund Raising

Cyber crime has increased in past years, and several recent terrorist events appear to have been funded partially through online credit card fraud. Extremist hackers have reportedly used identity theft and credit card fraud to support terrorist activities by Al Qaeda cells. When terrorist groups do not have the internal technical capability, they may hire organised crime syndicates and cybercriminals through underground digital chat rooms. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists’ desire to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

Cyberattacks

Although terrorists have been adept at spreading propaganda and attack instructions on the web, it appears that their capacity for offensive computer network operations may be limited. The Federal Bureau of Investigation (FBI) reports that cyberattacks attributed to terrorists have largely been

limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites. However, it says, their increasing technical competency is resulting in an emerging capability for network-based attacks.

The FBI has predicted that terrorists will either develop or hire hackers for the purpose of complementing large conventional attacks with cyberattacks. During his testimony regarding the 2007 Annual Threat Assessment, FBI Director Robert Mueller observed that “terrorists increasingly use the Internet to communicate, conduct operational planning, proselytise, recruit, train and to obtain logistical and financial support. That is a growing and increasing concern for us.” In addition, continuing publicity about Internet computer security vulnerabilities may encourage terrorists’ interest in attempting a possible computer network attack, or cyberattack, against U.S. critical infrastructure. The Internet, whether accessed by a desktop computer or by the many available handheld devices, is the medium through which a cyberattack would be delivered. However, for a targeted attack to be successful, the attackers usually require that the network itself remain more or less intact, unless the attackers assess that the perceived gains from shutting down the network entirely would offset the accompanying loss of their own communication. A future targeted cyberattack could be effective if directed against a portion of the U.S. critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, radiological, or nuclear (CBRN) terrorist attack.

The objectives of a cyberattack may include the following four areas:

1. loss of integrity, such that information could be modified improperly;
2. loss of availability, where mission-critical information systems are rendered unavailable to authorised users;
3. loss of confidentiality, where critical information is disclosed to unauthorised users; and

4. physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Publicity would also potentially be one of the primary objectives for a terrorist cyberattack. Extensive media coverage has shown the vulnerability of the U.S. information infrastructure and the potential harm that could be caused by a cyberattack. This might lead terrorists to believe that even a marginally successful cyberattack directed at the United States would garner considerable publicity.

Some suggest that were such a cyberattack by an international terrorist organization to occur and become known to the general public, regardless of the level of success of the attack, concern by many citizens and cascading effects might lead to widespread disruption of critical infrastructures. For example, reports of an attack on the international financial system's networks could create a fiscal panic in the public that could lead to economic damage. According to security experts, terrorist groups have not yet used their own computer hackers nor hired hackers to damage, disrupt, or destroy critical infrastructure systems.

Yet reports of a recent disruptive computer worm that has spread through some government networks, including that of the National Aeronautics and Space Administration, have found a possible link to a Libyan hacker with the handle "Iraq Resistance" and his online hacker group "Brigades of Tariq ibn Ziyad," whose stated goal is "to penetrate U.S. agencies belonging to the U.S. Army." References to both the hacker and group have been found in the worm's code. However, this does not provide conclusive evidence of involvement, as e-mail addresses can be spoofed and code can be deliberately designed to implicate a target while concealing the true identity of the perpetrator.

The recent emergence of the Stuxnet worm may have implications for what potential future cyberattacks might look like. Stuxnet is thought to be the first piece of malicious software (malware) that was specifically designed to target the computer-networked industrial control systems that control

utilities, in this case nuclear power plants in Iran. Although many experts contend that the level of sophistication, intelligence, and access required to develop Stuxnet all point to nation states, not only is the idea now in the public sphere for others to build upon, but the code has been released as well. An industrious group could potentially use this code as a foundation for developing a capability intended to degrade and destroy the software systems that control the U.S. power grid, to name one example.

FEDERAL GOVERNMENT EFFORTS TO ADDRESS CYBER TERRORISM

A number of U.S. government organizations appear to monitor terrorist websites and conduct a variety of activities aimed at countering them. Given the sensitivity of federal government Programmes responsible for monitoring and infiltrating websites suspected of supporting terrorism-related activities, much of the information regarding the organizations and their specific activities is deemed classified or law enforcement-sensitive and is not publicly available. The information listed below represents a sampling of what has been publicly discussed about some of the federal government organizations responsible for monitoring and infiltrating jihadist websites.

It should be noted that the actions associated with the organizations listed below could be conducted by employees of the federal government or by civilian contract personnel.

- *Central Intelligence Agency (CIA):* development, surveillance, and analysis of websites, commonly referred to as honey pots, for purposes of attracting existing and potential jihadists searching for forums to discuss terrorism-related activities.
- *National Security Agency (NSA):* surveillance of websites and rendering them inaccessible.
- *Department of Defence (DOD):* surveillance of websites focused on discussions of perceived vulnerabilities of overseas U.S. military facilities or operational capabilities and disabling those that present a threat to operations.

- *Department of Justice (DOJ)*: development of policies and guidelines for creating, interacting within, surveilling, and rendering inaccessible websites created by individuals wishing to use the Internet as a forum for inciting or planning terrorism-related activities.
- *Federal Bureau of Investigation (FBI)*: monitoring of websites and analysis of information for purposes of determining possible terrorist plans and threats to U.S. security interests.
- *Department of Homeland Security (DHS)*: monitoring of websites and analysis of information for purposes of determining possible threats to the homeland.

Numerous other federal government organizations have cyber security responsibilities focused on policy development, public awareness campaigns, and intergovernmental and private sector coordination efforts. Information gleaned from the agencies may at times be used to help inform and advise non-federal government entities responsible for safeguarding a geographic area or activity that has been discussed in an online jihadist forum.

Federal Government Monitoring and Response

A number of reasons exist that may provide justification for the federal government to monitor websites owned, operated, or frequented by individuals suspected of supporting international jihadist activity that pose a threat to U.S. security interests.

Such websites may be used for purposes of spreading propaganda, recruiting new members or enticing existing participants, communicating plans counter to U.S. interests, or facilitating terrorist-related activities. Quite often the jihadist websites are the first indicators of extreme elements of the jihadist community identifying a controversial issue for purposes of inciting action harmful to U.S. interests. For example, a recent controversy in the United States about a proposed burning of copies of the Quran on the ninth anniversary of the September 11, 2001, attacks led to increased chatter on international jihadist websites. The FBI reportedly

disseminated an intelligence bulletin specifically noting online threats to the pastor and church planning to conduct this event and more general threats to U.S. global interests. When assessing whether to monitor, infiltrate, or shut down a Web site suspected of inciting participants to take harmful actions against U.S. security interests, numerous competing interests should be considered. First, the federal government would determine whether the Web site is owned by a U.S. corporation and whether U.S. citizens may be participating in the Internet forum. Such a determination is necessary to ensure that proper procedures are adhered to with respect to upholding the rights afforded by the U.S. Constitution's First and Fourth Amendments, in particular.

Second, once it is confirmed that a suspected jihadist Web site is being used to facilitate terrorism-related activities, the national security community may consider the short- and long-term implications of a variety of operational responses. Options include permanently or temporarily shutting down the Web site, passively monitoring the Web site for intelligence-gathering purposes, or covertly engaging the members of the forum with the desire to elicit additional information for purposes of thwarting a potential terrorism-related activity and/or building a stronger criminal case. Different agencies may weigh each option differently, creating a need to achieve interagency consensus prior to action.

DOD has been considering establishing a computer network monitoring database for government and private networks. Organizations would provide information on a voluntary basis, and the data collected would be shared with all participants. However, privacy concerns and questions of DOD's proper role in federal cyber security make the implementation of such a Programme unlikely in the current political climate.

A memorandum of agreement signed in October 2010 between DHS and DOD represents an effort to increase coordination of operations and plans to protect civilian critical infrastructure as well as military networks. The partnership could be used as a means through which DOD

would have a greater role in defending privately owned critical infrastructure using the EINSTEIN 2 and 3 network monitoring systems developed by DHS.

Counterpropaganda

In common parlance and in media reporting, the terms “strategic communications,” “public diplomacy,” “global engagement,” “information operations,” and “propaganda” are often used interchangeably. This confusion in terms makes it difficult to determine exactly what sorts of programmatic activities are being discussed. There is no overarching definition of strategic communications for the federal government.

DOD has defined strategic communication as “focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States government interests, policies, and objectives through the use of coordinated Programmes, plans, themes, messages, and products synchronised with the actions of all instruments of national power.” This term, as defined, describes a U.S. government-wide process, not an organizational structure, capability, or discrete activity within DOD or any other government agency.

As prescribed by the 2009 National Framework for Strategic Communication, the Deputy National Security Advisor for Strategic Communications (DNSA/SC) serves as the National Security Advisor’s principal advisor for strategic communications. The Senior Director for Global Engagement (SDGE) is the principal deputy to the DNSA/SC.

Together, they are responsible for ensuring that

- The message-value and communicative impact of actions are considered during decision-making by the National Security Council (NSC) and Homeland Security Council (HSC);
- The mechanisms to promote strategic communication are in place within the National Security Staff (NSS); and

- Similar mechanisms are developed across the interagency.

The DNSA/SC and SDGE are also responsible for guiding and coordinating interagency deliberate communication and engagement efforts, and they execute this responsibility through the NSS Directorate for Global Engagement (NSS/GE) and through the Interagency Policy Committee (IPC) on Strategic Communication. Public Diplomacy (PD) within the State Department is led by the Under Secretary for Public Diplomacy and Public Affairs.

The Department of State distinguishes between Public Affairs (PA), which includes outreach to domestic publics, and PD—which seeks to promote the national interest of the United States through understanding, engaging, informing, and influencing foreign publics, and by promoting mutual understanding between the people of the United States and people from other nations around the world. In DOD, strategic communication-related activities are primarily supported by the integration of three capabilities: Information Operations (IO), and, primarily within IO, Psychological Operations (PSYOP), Public Affairs (PA), and Defence Support to Public Diplomacy (DSPD). Military Diplomacy (MD) and Visual Information (VI) also support strategic communications-related activities.

DOD sees strategic communications as a process to synchronise efforts that:

- Improve U.S. credibility and legitimacy;
- Weaken an adversary's credibility and legitimacy;
- Convince selected audiences to take specific actions that support U.S. or international objectives;
- Cause a competitor or adversary to take (or refrain from taking) specific actions.

Many DOD activities support the State Department's public diplomacy efforts and objectives, which in turn support national objectives. DOD refers to these activities as "Defence Support to Public Diplomacy" (DSPD). Although some reports warn of social media's potential misuse by terrorists, government policies are evolving to embrace the use of tools

such as Facebook and Twitter as a means of strategic communications and public diplomacy. On the one hand, social media tools such as Twitter and Facebook can be used by terrorist groups to expand networks and exchange real-time information, enabling operatives to organise and act quickly. These tools can not only spread propaganda, but can also host embedded malicious software in links and applications that can corrupt an unsuspecting user's electronic device.

Based on these security concerns, several services and offices within DOD had banned certain social networking sites from access on their unclassified networks. However, the federal government has begun to embrace using these same tools to allow free access to information, spread democratic values and ideas, and combat the misinformation spread by terrorist groups' media campaigns. In February 2010, DOD issued a directive-type memo (DTM) outlining the department's new social media policy, citing Internet-based capabilities including social networking services as integral to operations.

This policy is due to expire in March 2011; reportedly, there are no plans to develop a replacement policy, nor plans to fill the top positions that were instrumental in creating the social media policy. Some fear that the recent WikiLeaks issue may push the pendulum back Towards more restricted access to Internet-based capabilities and less information sharing between organizations.

Others note that, to date, much of the activity conducted under the current policy has been one-sided, focused on using social network tools to gather information about others, including potential adversaries, rather than to send messages outward in order to shape the information environment. Reportedly, the U.S. Air Force and U.S. Central Command have been developing deceptive identities on the Internet in order to infiltrate chat rooms and other social media using a special software. The U.S., Air Force software contract states that it shall be used to target adversarial sites worldwide without detection, and spokesmen for the U.S. Central Command have stated that it shall not be used to target law-abiding American

citizens. Critics of these Programmes point to the potential loss of credibility, a tenet of successful information operations, using the former Office of Strategic Influence (OSI) as an example. Reports that the OSI was planting false news stories into foreign newspapers to gain support for the war in Iraq led many—including the Public Affairs Office—to question the legality of such activity. The OSI was subsequently disestablished.

Department of Defence Offensive Response

Information operations do not refer exclusively to messaging and content; another integrated capability within this area is computer network operations (CNO), which includes cyberattack capabilities, cyber espionage and exploitation, and cyber Defence. The Joint Functional Command Component—Network Warfare (JFCC-NW) and the JFCC—Space and Global Strike (JFCC-SGS) have responsibility for overall DOD cyber security, while the Joint Task Force—Global Network Operations (JTF-GNO) and the Joint Information Operations Warfare Center (JIOWC) both have direct responsibility for Defence against cyberattack.

The DOD focal point for coordinating military information operations is the JIOWC. The JTF-GNO defends the DOD Global Information Grid, while the JIOWC assists combatant commands with an integrated approach to information operations. These include operations security, military information support operations (formerly psychological operations), military deception, and electronic warfare. Many of the specific Programmes under the JIOWC's purview are classified.

The JIOWC also coordinates computer network operations and network warfare with the JTF-GNO and with JFCC-NW. These latter two organizational activities are to fall under the responsibility of the newly formed U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command (USSTRATCOM). The commander of USCYBERCOM, General Keith Alexander, also serves as the director of NSA. Traditionally, the NSA mission has been

information assurance for national security systems and signals intelligence, and gathering information about potential threats under the Foreign Intelligence Surveillance Act (FISA). The dual-hatted nature of this appointment places this intelligence function alongside the offensive operations command. Information security and cyberwarfare planners in the Pentagon have noted both in doctrine and in informal channels that a good offensive cyber operations capability is the best Defence.

For this reason, USCYBERCOM has integrated the military's defensive computer network operations components with its offensive arm under one joint command. Many of USCYBERCOM's capabilities are unknown, due to the classified nature of offensive cyber operations. There have also been questions in the executive branch and in Congress about what authorities they operate under and how oversight is to be conducted.

A question-and-answer exchange from the Senate Armed Services Committee revealed that DOD had not included cyber operations in its quarterly report on clandestine military activities. Michael Vickers, the nominee for Undersecretary of Defence for Intelligence, reportedly told the committee that those quarterly reporting requirements related only to human intelligence. How USCYBERCOM relates to NSA and how both relate to the private sector, which owns most of the U.S. telecommunications infrastructure, has been a continued subject of discussions.

On the defensive side, although USCYBERCOM is developing plans to defend the.mil domain, there is still no unified federal response policy for coordinating offensive cyber operations at the national level. Yet DOD has been working with DHS and the National Cyber security and Communications Integration Center through Cyberstorm and other exercises to map out a National Cyber Incident Response Plan, which gives a structure for how the federal government might respond in the event of a major cyberattack. At a Reserve Officers Association conference, USCYBERCOM Chief of Staff Major General David Senty said that the sub-unified command

might take the lead in defending the nation's military networks as a "supported command" prior to "turning things over" to U.S. Northern Command.

FEDERAL GOVERNMENT CHALLENGES AND IMPLICATIONS

Although organizations, policies, and plans exist to counter violent extremists' use of the Internet, implementation may be hampered by several factors. Laws may be interpreted by some agencies to prohibit certain activities, and in some cases agencies may have competing equities at stake.

Legislative and policy authority may be given to organizations that lack the technical capability to fulfill a mission, while entities with the capacity to address cyber attacks may be legally constrained from doing so due to privacy or civil liberties concerns. There may be tensions between the Global Internet Freedom Initiative as highlighted by Secretary of State Hillary Clinton and overall counterterrorism objectives. Additionally, the lack of clarity in definitions related to information operations and terrorism may lead to institutional questions such as which agency has the lead for federal government coordination or independent oversight.

Institutional Constraints

Some argue that the effectiveness of the U.S. government's strategic communications, information operations, and global engagement Programmes is still hampered by the U.S. Information and Educational Exchange Act of 1948, also known as the Smith-Mundt Act. The law directs that information about the United States and its policies intended for foreign audiences "shall not be disseminated within the United States, its territories, or possessions."

Amendments to the Smith-Mundt Act in 1972 and 1998 further clarified the legal obligations of the government's public diplomacy apparatus, and several presidential directives, including NSPD-16 in July 2002, have set up specific structures and procedures as well as further legal restrictions regarding U.S. public diplomacy and information operations. Some say

that these policies have created an unnecessary “firewall” between domestic and foreign audiences, limiting what information the United States produces and distributes to counter extremists in cyberspace for fear of “blow-back” to its own citizens. Cyberspace as a global domain does not recognise territorial boundaries, making it difficult to target a specific geographic region. Some argue that this has effectively created a ban on all government “propaganda,” a term that carries with it negative historical connotations, although the term is neither defined nor mentioned in the law itself.

Some critics argue that the law does not prevent government propagandizing, but rather has been consistently misinterpreted. Others maintain that the Smith-Mundt provisions may prevent undue government manipulation of citizens and are a necessary protection. In addition to questions over what constitutes propaganda and the applicability of Smith-Mundt, confusion over “information operations” Programmes has led some to question their budgetary process and management within DOD.

Often confused with Information Operations as a whole, PSYOP refers to influence activities specifically intended “to induce or reinforce foreign attitudes and Behaviour in a manner favorable to U.S. objectives.” While PSYOP is focused at audiences abroad, it is supported by the public affairs function. The Public Affairs Office (PAO) is the entity responsible for working with media outlets both domestic and foreign, to “inform” rather than to “influence.”

Given the public’s and government’s aversion to the term “propaganda” and particularly military activities that might be described as such, DOD has changed military lexicon from PSYOP to Military Information Support Operations (MISO). The Secretary of Defence approved the name change in June 2010 following a recommendation from the Defence Senior Leadership Council. Some argue that the name change elevates the importance of information support to military operations for commanders in the field, while others point to the traditional career field of PSYOP as a source of pride among its servicemembers. A January 2011 memorandum issued by

DOD acknowledges the heightened strategic emphasis on countering violent extremism and transnational, global networks through effective strategic communications and information operations. The memo outlines organizational changes that are designed to facilitate better Programme integration and coordination to meet these challenges.

The new construct places the JIOWC under the Joint Staff in all but its electronic warfare coordinating function, which shall still remain the purview of USSTRATCOM. The memo also describes new requirements for resource managers to capture the costs of MISO and to develop standardised budget methodologies for SC and IO capabilities and activities. This is in response to congressional concerns over what constitutes an "information operation" and how much federal money is spent on what has been perceived as military propaganda. The Department of Defence Appropriations Acts for FY2002 through FY2010 provide that, "No part of any appropriation contained in this Act shall be used for publicity or propaganda purposes not authorised by the Congress."

Title 10 of the *United States Code*, Section 167, authorises combatant commanders to conduct psychological operations as part of clandestine special operations campaigns in support of military missions. However, Title 10 does not define PSYOP, nor does it clarify DOD's authority to conduct information operations versus propaganda. Some private U.S. citizens have attempted to work outside of these institutional constraints. For instance, inspired by 9/11, Montana resident Shannen Rossmiller has been using the Internet to glean information about potential terrorist suspects and their plans.

This information, which she has shared with federal intelligence agencies, has led to the arrests of a Washington state National Guardsman, convicted in 2004 of attempted espionage for plans to transmit U.S. military armor information through the Internet, and a Pennsylvania man who prosecutors say sought to blow up oil installations in the United States. As a self-taught private citizen, Ms. Rossmiller can operate outside of the institutional constraints that may bind federal employees. Rita Katz of Search for International Terrorist Entities (SITE

Institute) performs similar activities, funneling intelligence mined from online extremist chat rooms to government officials without having to go through the sometimes onerous and time-consuming official channels. The intelligence agencies have not discussed publicly the nature of the information shared, nor how it was used.

Intelligence Gain/Loss Calculus

Tensions between a website's purported intelligence value and operational threat level can determine the particular capabilities used to thwart the site. For example, a "honey pot" jihadist Web site reportedly was designed by the CIA and Saudi Arabian government to attract and monitor terrorist activities. The information collected from the site was used by intelligence analysts to track the operational plans of jihadists, leading to arrests before the planned attacks could be executed. However, the Web site also was reportedly being used to transmit operational plans for jihadists entering Iraq to conduct attacks on U.S. troops. Debates between representatives of the NSA, CIA, DOD, DNI, and NSC led to a determination that the threat to troops in theater was greater than the intelligence value gained from monitoring the Web site, and a computer network team from the JTF-GNO ultimately dismantled it. This case raised questions of whether computer network attacks on a Web site are a covert operation or a traditional military activity, and under what authority they are conducted. It also illustrated the risk of collateral damage that an interconnected, networked world represents, as the operation to target and dismantle the honey pot inadvertently disrupted servers in Saudi Arabia, Germany, and Texas. Also, some point to the potential futility of offensively attacking websites, as a dismantled site may be easily relocated to another server. The 2010 National Security Strategy mentions the importance of the Internet for commerce and for disseminating information, and the importance of cyber security in protecting national security assets, but does not appear to present a strategy specifically for combating violent extremism on the Internet.

A number of hearings have been held to address the issue of violent extremism on the Internet. In a March 2, 2010, "Dear Colleague" letter, members of the House of Representatives announced the formation of a new Strategic Communications and Public Diplomacy Caucus, whose stated purpose is to "raise awareness of the challenges facing strategic communication and public diplomacy and provide multiple perspectives on proposed solutions."

On July 13, 2010, the caucus's chairs, Representatives Mac Thornberry and Adam Smith, introduced H.R. 5729, the Smith-Mundt Modernization Act of 2010. This measure would amend the United States Information and Educational Exchange Act of 1948 to allow the Secretary of State to create products designed to influence audiences abroad that could also be disseminated domestically, thereby removing the "firewall." Another piece of legislation introduced in the 111 Congress was S. 3480, the Protection of Cyberspace as a National Asset Act.

This bill, which may be reintroduced in some form in the current Congress, has generated much discussion over what some describe as the "Internet Kill Switch." Recent events of social unrest and government Internet control in the Middle East highlight the question of whether the President has the authority to "turn off" the U.S. connection to the Internet in times of similar crisis and whether such authority is needed. Critics consider such a communication disruption as an attack on the freedom of speech and the free flow of information.

Others point to the economic damage that could result from the loss of networked communications. Regardless, blocking the flow of traffic into and out of U.S. information infrastructure would require the assistance of many private Internet service providers (ISPs), as there is no single, government-owned national network. The bill's sponsors wrote that such authorities already exist for the President to compel private companies to suspend service, particularly in the Communications Act of 1934, and the new legislation would

actually limit presidential emergency powers over the Internet. A new proposal in the 112 Congress, S. 413, the Cyber security and Internet Freedom Act of 2011, contains a provision that would amend the Communications Act of 1934 so that, “[n]otwithstanding any provision of this Act, an amendment made by this Act, or section 706 of the Communications Act of 1934, neither the President, the Director of the National Center for Cyber security and Communications, or any officer or employee of the United States Government shall have the authority to shut down the Internet.” The Communications Decency Act of 1996 (CDA), codified in Title V of the Telecommunications Act of 1996, was an effort to regulate both indecency and obscenity in cyberspace.

Although much of it is targeted at lewd or pornographic material, particularly when shown to children under the age of 18, the law’s definition of obscenity and harassment could also be interpreted as applying to graphic, violent terrorist propaganda materials or incendiary language. YouTube’s terms of use (called “Community Guidelines”) prohibit, among other things, “gratuitous and graphic violence” and “hate speech.” To control its content, YouTube employs a user-feedback system, where users flag potentially offensive videos that are then reviewed and removed by the site’s administrators. However, Section 230 of the CDA reads: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

This would absolve both ISPs and Internet administrators from liability for the words or crimes committed by third-party users of their websites or online forums, even if the provider or administrator fails to take action after receiving notice of the harmful or offensive content. In other words, although many ISPs and Web site administrators follow internal policies that restrict the type of material posted on their sites or trafficked through their networks, they may not have a legal responsibility to dismantle a site with offensive or violent content. In September 2010, General Alexander told the House Armed Services Committee that the White House was leading

an effort to review the legal framework governing operations in cyberspace and the protection of telecommunications infrastructure. The results of this review will be presented to Congress, with legislative recommendations on what new statutes may be required and which should be revised or amended to facilitate effective operations in cyberspace. The 2011 National Military Strategy also contains a point to that effect.

Chapter 5

Hacking

Hacking means finding out weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground but it is now an open community. While other uses of the word hacker exist that are not related to computer security, they are rarely used in mainstream context. They are subject to the long standing hacker definition controversy about the true meaning of the term hacker. In this controversy, the term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

CLASSIFICATION

Several subgroups of the computer underground with different attitudes use different terms to demarcate themselves from each other, or try to exclude some specific group with which they do not agree. Eric S. Raymond (author of *The New Hacker's Dictionary*) advocates that members of the computer underground should be called crackers. Yet, those people see themselves as hackers and even try to include the views of Raymond in what they see as one wider hacker culture, a view harshly rejected by Raymond himself. Instead

of a hacker/cracker dichotomy, they give more emphasis to a spectrum of different categories, such as white hat, grey hat, black hat and script kiddie. In contrast to Raymond, they usually reserve the term cracker for more malicious activity. According to a cracker or cracking is to "gain unauthorised access to a computer in order to commit another crime such as destroying information contained in that system". These subgroups may also be defined by the legal status of their activities.

White Hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, also known as the International Council of Electronic Commerce Consultants has developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.

Black Hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorised to use the network. They choose their targets using a two-pronged process known as the "pre-hacking stage".

- *Part 1: Targeting:* The hacker determines what network to break into during this phase. The *target* may be of particular interest to the hacker, either politically or personally, or it may be picked at random. Next, they will port scan a network to

determine if it is vulnerable to attacks, which is just testing all ports on a host machine for a response. Open ports—those that do respond—will allow a hacker to access the system.

- *Part 2: Research and Information Gathering:* It is in this stage that the hacker will visit or contact the target in some way in hopes of finding out vital information that will help them access the system. The main way that hackers get desired results from this stage is from “social engineering”, which will be explained below. Aside from social engineering, hackers can also use a technique called “dumpster diving”. Dumpster diving is when a hacker will literally search through users’ garbage in hopes of finding documents that have been thrown away, which may contain information a hacker can use directly or indirectly, to help them gain access to a network.
- *Part 3: Finishing The Attack:* This is the stage when the hacker will invade the preliminary target that he/she was planning to attack or steal. Many “hackers” will be caught after this point, lured in or grabbed by any data also known as a honeypot (a trap set up by computer security personnel).

Grey Hat

A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.

Elite Hacker

A social status among hackers, *elite* is used to describe the most skilled. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

A script kiddie (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).

Neophyte

A neophyte, “n00b”, or “newbie” is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Blue Hat

A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Hacktivist

A hacktivist is a hacker who utilises technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves Web site defacement or denial-of-service attacks.

ATTACKS

A typical approach in an attack on Internet-connected system is:

- *Network enumeration:* Discovering information about the intended target.
- *Vulnerability analysis:* Identifying potential ways of attack.
- *Exploitation:* Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

Security Exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in Web site/domain hacking.

Techniques

- *Vulnerability scanner*: A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what Programme or service is listening on that port, and its version number.
- *Password cracking*: Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.
- *Packet sniffer*: A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.
- *Spoofing attack (Phishing)*: A spoofing attack involves one Programme, system, or Web site successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another Programme. The purpose of this is usually to fool Programmes, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

- *Rootkit*: A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of Programmes which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.
- *Social engineering*: When a Hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system. Hackers who use this technique have to be quite savvy and choose the words they use carefully, in order to trick the system administrator into giving them information. In some cases only an employed help desk user will answer the phone and they are generally easy to trick. Another typical hacker approach is for the hacker to act like a very angry supervisor and when the his/her authority is questioned they will threaten the help desk user with their job. Social Engineering is so effective because users are the most vulnerable part of an organization. All the security devices and Programmes in the world won't keep an organization safe if an employee gives away a password. Black Hat Hackers take advantage of this fact. Social Engineering can also be broken down into four sub-groups. These are intimidation, helpfulness, technical, and name-dropping.
 - *Intimidation*: With the angry supervisor, the hacker attacks the person who answers the phone with threats to their job. Many people

at this point will accept that the hacker is a supervisor and give them the needed information.

- *Helpfulness*: Opposite to intimidation, helpfulness is taking advantage of a person natural instinct to help someone with a problem. The hacker will not get angry instead act very distressed and concerned. The help desk is the most vulnerable to this type of Social Engineering, because they generally have the authority to change or reset passwords which is exactly what the hacker needs.
- *Name-Dropping*: Simply put, the hacker uses the names of advanced users as “key words”, and gets the person who answers the phone to believe that they are part of the company because of this. Some information, like web page ownership, can be obtained easily on the web. Other information such as president and vice president names might have to be obtained via dumpster diving.
- *Technical*: Using technology to get information is also a great way to get it. A hacker can send a fax or an e-mail to a legitimate user in hopes to get a response containing vital information. Many times the hacker will act like he/she is involved with law enforcement and needs certain data for record keeping purposes or investigations.
- *Trojan horses*: A Trojan horse is a Programme which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with conceptually similar function of deceiving defenders into bringing an intruder inside.)

- *Viruses*: A virus is a self-replicating Programme that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes most computer viruses are considered malicious.
- *Worms*: Like a virus, a worm is also a self-replicating Programme. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing Programme. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating Programme.
- *Keyloggers*: A keylogger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some keyloggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a keylogger on a computer used at a point of sale and data collected by the keylogger could be used for catching employee fraud.

Chapter 6

Spam Attacks

INTRODUCTION

Nowadays, E-mail (Electronic mail) communication plays a great role in the human life due to its fast and free availability, lower or free cost. It is more useful for many corporate because of some features like newsletters, business correspondence, E-mail marketing, Advertisements etc. Like Freelancer.com Support use e-mail service for business correspondence to send the emails and messages to its authorised members.

Google news alerts use it for the newsletter. Naukri.com, DevNetworkIndia.org and etc. use e-mail service for the new jobs advertisements massively. Inkfruit, ZoomIn, Fashnvia.com (India) and etc. use e-mail service for their product marketing and their advertisements. Many times, these mails like Product advertisements, job advertisements, news alerts are meaningful for the e-mail users but sometimes, they generate spam mails over the mail-inbox.

Today, E-mail and chat services are the most common, instantaneous and successful Internet applications, which are threatened by spam mails and spam chats. These Service can be accessed using mobile Internet or low speed Internet. Spam mails can be an advertisement or notification of porn Web site, porn video, phishing Web site, Nigerian scam, medicines advertisements, adult content etc.

Spammers collect e-mail addresses from chatrooms, public networking websites, customer lists, newsgroups, and worms, viruses which harvest users' address books, and are

sold to other spammers. They also use a practice known as “e-mail appending” or “epending” in which they use known information about their target (such as a postal address) to search for the target’s e-mail address. Much of spam is sent to invalid e-mail addresses.

Spam averages 78 per cent of all e-mail sent. The spam detection problem seems more serious over mailboxes today. Without a spam filter, one e-mail user might receive over hundreds of mails daily and find that most of them are of spam category.

Spam mails consume unnecessary traffic over the Internet as well as e-mail service provider. Moreover, receiving spam mails are with no use for e-mail users. In the employed system, a highly simplified architecture of artificial neural networks is used to detect the misbehaviour of incoming mails.

An artificial neural network is a mathematical model which works on the principles of biological neural networks. Generally it is referred as neural network (NN). Using neural network model; we can easily map the complex inputs with the complex outputs.

Some of the silent features of ANN are as follows:

- They represent a highly connected network of neurons - the basic processing unit.
- They operate in a highly parallel manner.
- Each neuron does some amount of information processing.
- It derives inputs from some other neuron and in return gives its output to other neuron for further processing.
- This layer-by-layer processing of the information results in great computational capability.
- As a result of this parallel processing, ANNs are able to achieve great results when applied to real-life problems.

A typical architecture of neural network is depicted in figure.

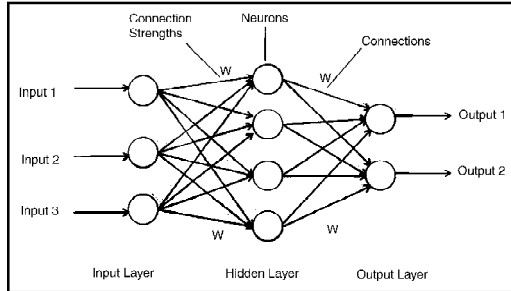


Fig. Architecture of Neural Network.

Neural network performs its operations in two phases: learning phase and testing phase.

Learning Phase

In the proposed methodology, we have taught several SQL attacks to the network in a supervised manner. We entrust the system with several variants of any attack and assign it a particular *label*.

Thus we can see that system learns by feeding various patterns of the same attack. During the *training process of neural network*, matrix of inbox mails and spam mails is used as input matrix to the neural network. In the proposed methodology, the input matrix is updated after defined time interval. Any neural network adjusts the weights of attacks in order to learn in a supervised or unsupervised manner.

In our method of learning, each candidate attack taught to the network is associated with a weight matrix. Weight matrix associated with the k th spam is assigned the label W_k . Weight matrix is updated with the progress of the learning of the spam mail.

This matrix is initialised to zero when learning phase starts. An input pattern corresponding to the spam is taught to the submitted to the network.

According to information compiled by Commtouch Software Ltd., E-mail spam for the first quarter of 2010 can be broken down as follows.

Table. E-mail Spam by Topic.

Pharmacy	81%
Replica	5.40%
Enhancers	2.30%
Degrees	1.30%
Casino	1%
Phishing	2.30%
Weight Loss	0.40%
Other	6.30%

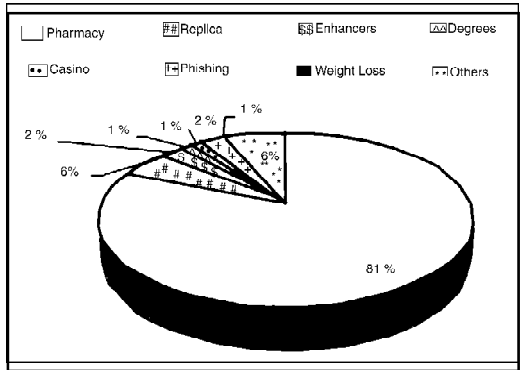


Fig. Spam e-mails Distribution by Topic.

Due to following characteristics, currently the identification process of spam mails is a difficult problem.

- Spam heterogeneity
- Spam definition

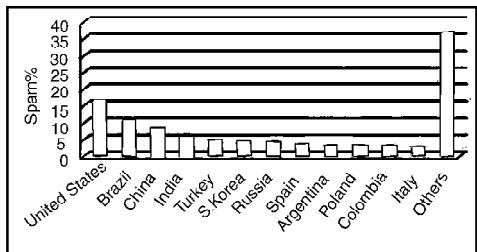


Fig. Represents the Spam Distribution over Various Countries.

By continent, Asia continues to dominate in spam, with more than a third of the world's unsolicited junk e-mail relayed

by the region. Asia covers 34.8 per cent spam mails over all the spam mails. The breakdown of spam relaying by continent is as follows.

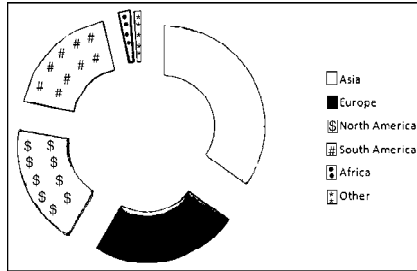


Fig. Spam Distribution over Various Regions.

SPAMMER APPROACHES AND THEIR ATTACK

There are many techniques adopted by the spammer or attackers to collect and store the e-mail addresses or personal information etc. Some of those approaches are from posts to UseNet with e-mail address, from mailing lists, from web pages, from various web and paper forms, via an Ident daemon, from a web browser, from IRC and chat rooms, from finger daemons, from AOL profiles, from domain contact points, by guessing and cleaning, from white and yellow pages, from a previous owner of the e-mail address, by having access to the same computer, using social engineering, from the address book and emails on other people's computers, buying lists from others, by hacking into sites and etc.



Fig. A Spam Box Folder Over the Mailbox.

With a marketing service, a person can arrange his contacts by certain demographics so that he can create custom mailing lists. This means that he can have some newsletters that go to all customers while also having some that only go to women or men or people with a history of shopping in a particular category.

These tailored mailing lists ensure that your messages are only received by customers who may be interested in the subject matter, keeping those who likely would not be from feeling as though they are being spammed and unsubscribing. Currently, a lot of social networking sites exists over WWW. Some sites are really useful but some creates spam mails over the mailbox.

With social networking sites, when a person joins some social networking Web site (like shtyle.fm, yaari.com, indiarocks.com, mycantos.com, facebook.com, tagged.com etc.), then these social site use some script to approach contacts (contact mail list) of that person and send invitation to his contacts to join the same social site. Many times they fill spam mails in peoples' inbox using this approach. There are also many several attacks over the mailbox by the spammers. Some spammers generate spam mails over the mailbox using the manual script but some use machine generated scripts to generate the spam mails.

RELATED WORK

In literature, there are many techniques described for the detection of spam and mail filtering. Some of the techniques are described as follows: A Rule approach has been proposed for the detection of spam mails. The discussed approach uses the training and testing phases of data. Moreover, the stale and obsolete spam rules suspend during the training.

This action is used for improving the spam filtering efficiency. However, the time complexity is higher due to the rules generation and their execution. E. Damiani *et al.* discussed some basic properties of the spam mails. They focused on the reasons of the popularity of spam mails. The uses of the digests in the proposed approach to identify spam

mails in a privacy-preserving way is a fundamental technique for collaborative filtering. A social network is constructed based on e-mail exchanges between various users. Spammers are identified by observing abnormalities in the structural properties of the network.

Many times spammer uses the public social sites for increasing their mail list database. However, it is a reactive mechanism since spammers are identified after they have already sent spam. In a novel approach has been discussed, which creates a Bayesian network out of e-mail exchanges to detect spam. Though Bayesian classifiers can be used for detecting spam e-mails, they inherently need to scan the contents of the e-mail to compute the probability distributions for every node in the network.

Since many times it is not possible, to detect spam mails for the particular inbox and its requirement for filtering the spam mails. Nitin Jindal *et al.* discussed an approach of review spam. Review spam is quite different from Web page spam and e-mail spam, and thus requires different detection techniques.

There is an effective technique to detect the spam mail that is 'Fast Effective Botnet Spam Detection'. It uses the header information of mails to detect the spam mails. It is useful for both 'Text based spam' as well as 'image based spam'. It analyses the sender IP address, sender e-mail address, MX records and MX hosts. One approach is also described to detect the spam mails, it use the Bayesian calculation for single keyword sets and multiple keywords sets, along with its keyword contexts to improve the spam detection.

PROPOSED METHODOLOGY

Before proposing a new methodology for spam detection, we are aware of this fact that most of time spam mails and scams are spread out using the machine generated script. In this paper, we are proposing a new query based cross layer approach for the above that is based on the above facts and some other spam features. Our system uses some knowledge base and query generation using the history of previous mails

and spam mails which is specific for the each user or its mailbox. Using the knowledge base, detection of spam mails is performed. It also maintains some keywords list, which can easily be pointed out as some words or content in the incoming mail, then perform the detection operation. Many times when a person clicks a URL which is present in his mailbox, (that URL has been provided by the spammers) then mail address of the person is captured by the spammer and is easily inserted in spammer's database. Proposed spam detection approach, follow the few steps to indentify the spam mails.

Analyse the Mail Content

Firstly, proposed approach analyse the mail content and sender mail address of the mail, then cross analyse and compare the content and sender address of the previous spam mails if content and sender address both are already present in any of the previous spam mails then it directly declares the mail as "*a spam*" (a spam is already present with the same sender and same mail content). If the some fraction of incoming mail content matches with the any previous spam mail then mail is filtered using the spam threshold value (St). The spam threshold value can be defined as the mathematical value which decides the performance and accuracy of spam detection system. It can be different for various systems.

It is used to indentify the spam mails with the partially matching case.

- If $St = 0.7$ and matching fraction of the content of mail matches with the previous declared spam mails is greater than equal to 0.7, then the mail is declared as "*a spam*".
- *Matching fraction of the content* = $\max.(NM1/N1, NM2/N2, \dots, NMp/Np)$.
- NMp : Total number of exactly matched words of incoming mail with the pth spam mail.
- Np : Total number of words in p-th spam mail.
- P : The total no. of recent mails which are available in the spam mail list corresponding to that user.

Using the analysis step, following mail from PHP-classes

is detected as spam mail because it was already present in the spam folder and user never communicated with the sender mail id.

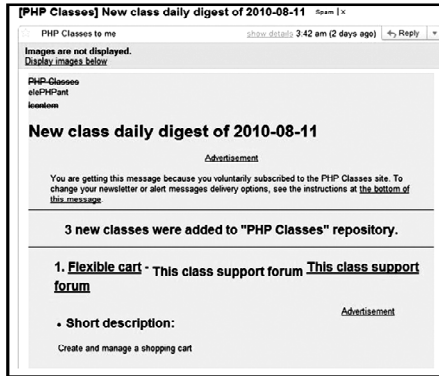


Fig. A Spam mail from the PHP Classes.

Trusted Knowledge Base

Knowledge Base is always a good, efficient and faster approach to give the results based on historical data. It is used some queries to execute the results. It also follow some update operation to make the result efficient based on the system requirements. In the Trusted Knowledge Base, database of trusted sender is stored over the inbox based on the frequency of the communication of mails. The Knowledge Base is also updated upon the requirement of inbox or threshold count of incoming mails. This Knowledge Base is responsible to the detection of spam mails when sender of incoming is already kept in the trusted zone. If the sender is not the trusted sender then next steps would be executed to indentify the spam mails.

Keywords knowledge Base

To execute this step, A knowledge base is maintained at mail server for each user which stores the spam keywords (already defined by the specific user). During this step, proposed approach analyses the keywords of mails with the keywords knowledge base of spam which is prepared by the particular user for detection of spam. Using the result it decides

that incoming mail belongs to the spam category or not. If incoming mail has not been declared as "*spam*" then execute the other steps to identify the spam mails.

Sender Mail Address

Our proposed methodology extract the sender mail address using the mail header (check the *from* field or *reply-to* field to get the sender e-mail address) and analyse it to identify the spam. Using the sender e-mail address, system finds that have any communication been done previously between receiver and sender or not? If receiver has already communicated with that mail address, then mail is declared as "*not a spam*". But if receiver has never communicated, then system explores the contact list of the receiver.

If the sender mail address already present in the contact list then the mail is declared as "*not a spam*".

This step is very useful with the public networking site because many times networking sites send invitation using someone contacts.

Sender Location

This step is useful when mail user receive a mail from the another country which already belongs to the spam mail country. Our approach finds the sender mail server location and then compares the location with the spam mails location. Using this step, we are able to filter out some lottery spam and some Nigerian scams too. Using this step following mail is easily detected as spam mail because nation of mail inbox is INDIA and incoming mail server exists in US and receiver has never communicated with the US mail sender so it can be detected as spam mail. Many mail server use the sender location approach to identify the spam so they ask to the users country and location at the time of mail registration.

Misbehaviour of Incoming Mail

This step is executed using the artificial neural network. Artificial Neural Network (ANN) is a scientific discipline that is concerned with the design and development of

algorithms that allow computers to adapt their behaviour based on data. ANN automatically learns to recognise complex patterns and makes intelligent and efficient decisions based on data.

In the spam filtering ANN learns the complex pattern of mails and makes intelligent, efficient decisions based on the incoming mail. Proposed methodology executes training phase testing phase using sample set of the mailbox to complete this step.

During this step, we are able to predict any misbehaviour event of incoming mails; Machines generated mails, flood of mails over inbox. Misbehaviour can be predicted using the time factor, some sender mail address, some attacks. To detect the Misbehaviour, training phase is executed after each threshold value of incoming mail over inbox.

Cross-Validation

During this step, system will verify the sender that sender is a genuine human user or machine generated user using some cross request.

If the incoming mail is machine generated e-mail, it implies that sender is not human user. So the machine generated mails are not able to validate their identity. Most of the spam mails are detected during this step.

IMPLEMENTATION AND ANALYSIS

We have conducted the analysis of spam mails using the proposed methodology on some inboxes of different peoples. We have created the environment using some web technologies HTML, script languages, AJAX, XML and MySql tools for implementing the methodology.

We also applied some basic concepts of PHP, AJAX, MySQL and JavaScript from the references. Figure represents the diagrammatic representation of the proposed methodology.

Cybercrime: An Introduction

```
Delivered-To: vikas@decenttechnologies.org
Return-Path: <skoot@skoot.com>
Received: from skoi.mta10.skoot.com (mx198.skoot.com
[89.249.17.198])
  by mx.google.com with ESMTP id t10a1017262rvl.81.2010.04.14.19.41.23;
  Wed, 14 Apr 2010 19:41:23 -0700 (PDT)
Received: from skoi.mta101 (unknown [50.246.10.51])
  by skoi.mta10.skoot.com (Postfix) with ESMTP id AFA3B2ACDBC
  for <vikas@decenttechnologies.org>; Thu, 12 Mar 2010 02:41:22 +0000
(UTC)
MIME-Version: 1.0
From: SKoot <skoot@skoot.com>
Sender: SKoot <skoot@skoot.com>
To: "vikas@decenttechnologies.org" <vikas@decenttechnologies.org>
Reply-To: SKoot <skoot@skoot.com>
Date: 12 Mar 2010 02:41:22 +0000
Subject: A gift box - SKoot
Content-Type: multipart/&#x2013;
  boundary="=boundary_649061_ab7ef89d-fac4-4a36-bbca-0ea779a0dfbf"
Content-Transfer-Encoding: quoted-printable
Message-Id: <20100415024122.AFA3B2ACDBC@koi.mta10.skoot.com>
```

Fig. Extracted Mail Header of the Inbox "vikas@decenttechnologies.org".

```
Delivered-To: payal@decenttechnologies.org
Received: by 10.141.29.111 with SMTP id g11cs495657rvj;
  Tue, 6 Apr 2010 07:07:36 -0700 (PDT)
Received: from mr.google.com ([10.141.124.15])
  by 10.141.124.15 with SMTP id b15mr1285989rvn.0.1270562856003 (mum_hops = 1);
  Tue, 06 Apr 2010 07:07:36 -0700 (PDT)

MIME-Version: 1.0
Reply-To: =?UTF-8?B?4pmh4pmh0ZLimarguZPmsYnOtyTRkuKZqiAuLi+uLi4u?=@#x2013;
  <himanshi.s@gmail.com>
Sender: 13341802658969214797@mail.orkut.com
Received: by 10.141.124.15 with SMTP id b15mr1161613rvn.0.1270562855948; Tue,
  06 Apr 2010 07:07:36 -0700 (PDT)
```

Fig. Extracted mail header of the inbox "payal@decenttechnologies.org".

CONCLUSION AND LIMITATION

Our work is inspired by a situation of large number of spam mails over the mailbox, those we have easily encountered. We have recorded the incoming mail activities of various mail boxes of an university server over 4 months and analysed those mails to get the better results and better performance of spam filtering. From table data, we can all results of spam mails, inbox mails, false match easily for the given time period.

The experiment results provide the complete scenario of the problem and accuracy of spam detection. Our system indicated that the spam was filtered out with 98.17 per cent with 0.12 per cent false positive. Table represents the recorded data over the 4 months time period. Limitation of the proposed method is that it needs more hardware for the execution and higher memory space. So many times, it increases the workload of the mail server. So to implement the proposed methodology for large mail servers, we need intelligent mail servers which

are can be reduced the time complexity and provide better performance of spam filtering. So that we can easily manage higher computation load. Due to more hardware specification and higher computation load, the cost of implementation of proposed methodology is much higher.

Table. Represents the Data of Recorded Activities over Mailboxes.

Month	Apr, 2010	May, 2010	Jun, 2010	July, 2010
Inbox	15870	17961	18460	17123
Spam	4692	7234	7494	7031
False Match	83	43	23	29
Total Mail	19562	25195	25954	23157
% Spam	24.8%	28.7%	28.9%	30.4%
Caught				
% False Match	0.42%	0.17%	0.089%	0.099%

Chapter 7

The Challenges of Fighting Cyber Crime

Recent developments in ICTs have not only resulted in new cyber crimes and new criminal methods, but also new methods of investigating cyber crime. Advances in ICTs have greatly expanded the abilities of law enforcement agencies. Conversely, offenders may use new tools to prevent identification and hamper investigation.

OPPORTUNITIES

Law enforcement agencies can now use the increasing power of computer systems and complex forensic software to speed up investigations and automate search procedures. It can prove difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out easily, the identification of illegal pictures is more problematic. Hash-value based approaches are only successful if pictures have been rated previously, the hash value is stored in a database and the picture that was analysed was not modified. Forensic software is able to search automatically for child pornographic images by comparing the files on the hard disk of suspects with information about known images.

For example, in late 2007, authorities found a number of pictures of the sexual abuse of children. In order to prevent identification the offender had digitally modified the part of the pictures showing his face before publishing the pictures over the Internet. Computer forensic experts were able to unpick the modifications and reconstruct the suspect's face.

Although the successful investigation clearly demonstrates the potential of computer forensics, this case is no proof of a breakthrough in child-pornography investigation. If the offender had simply covered his face with a white spot, identification would have been impossible.



Fig. Pending copyright with Interpol.

GENERAL CHALLENGES

Reliance on ICTs

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e-mail communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services. The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue.

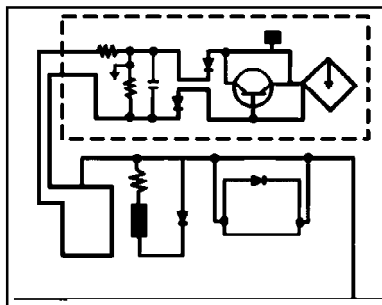


Fig. Information Technology and Electronic Devices are Increasingly Substituting Manual Functions.

Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures. Even

short interruptions to services could cause huge financial damages to e-commerce businesses - not only civil communications could be interrupted by attacks; the dependence on ICTs is a major risk for military communications. Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system, so offenders can design effective attacks by concentrating on this single target. The dependence of society on ICTs is not limited to the western countries - developing countries also face challenges in preventing attacks against their infrastructure and users. The development of cheaper infrastructure technologies such as WiMAX has enabled developing countries to offer Internet services to more people.

Developing countries can avoid the mistakes of some western countries that concentrated mainly on maximising accessibility, without investing significantly in protection. US experts explained that successful attacks against the official Web site of governmental organisations in Estonia could only take place due to inadequate protection measures. Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run. Strategies must be developed to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling the law enforcement to fight cyber crime effectively.

Number of Users

The popularity of the Internet and its services is growing fast, with over 1 billion Internet users worldwide. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware

and wireless access will enable even more people to access the Internet.

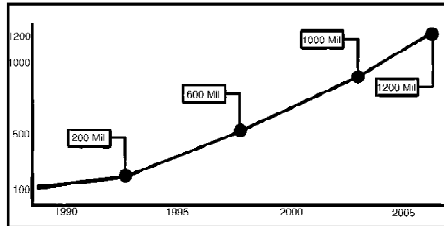


Fig. Currently there are more than 1 Billion Internet Users.

With the growing number of people connected to the Internet, the number of targets and offenders increases. It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million.

Although Internet usage rates are lower in developing countries, promoting cyber security is not easier, as offenders can commit offences from around the world. The increasing number of Internet users causes difficulties for the law enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can rather easily be carried out, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed was not modified.

Availability of Devices and Access

Only basic equipment is needed to commit computer crimes, which generally requires the following elements:

- Hardware;
- Software;
- Internet Access.

With regards to hardware, the power of computers grows continuously. There are a number of initiatives to enable people in developing countries to use ICTs more widely. Criminals

can commit serious computer crimes with only cheap or secondhand computer technology - knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cyber crimes. Committing cyber crime can be made easier through specialist software tools.

Offenders can download software tools designed to locate open ports or break password protection. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices.

The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialised countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so called "wardriving". The term describes the act of driving around searching for accessible wireless networks.

The most common way of access to network connections by offenders are:

- Public Internet terminals;
- Open (wireless) networks;
- Hacked networks;
- Prepaid services without registration requirements.

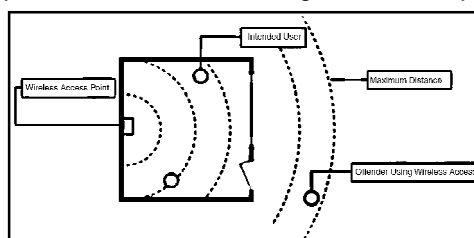


Fig. Access to the Internet without Leaving Traces is a High Priority for Many Offenders. The Graphic Shows how an Offender can use the Signal of an Open Wireless Network to Gain Remote Access. In These Cases, it is Almost Impossible to Identify the Offender.

Law enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users. However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigation of law enforcement agencies, such legislation could hinder the growth of the information society and development of e-commerce.

It has been suggested that this limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case *Autronic v. Switzerland*, the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

Availability of Information

The Internet has millions of webpages of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia, an online encyclopaedia where anybody can publish. The success of the Internet also depends on powerful search engines that enable the users to search millions of webpages in seconds.

This technology can be used for both legitimate and criminal purposes. "Googlehacking" or "Googledorks" describes the use of complex search engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password protection systems. Reports have highlighted the risk of the use of search engines for illegal purposes. An offender, who

plans an attacks can find detailed information on the Internet that explain how to build a bomb by using only those chemicals that are available in regular supermarkets. Although information like this was available even before the Internet was developed, it was however, much more difficult to get access to that information. Today any Internet user can get access to those instructions.

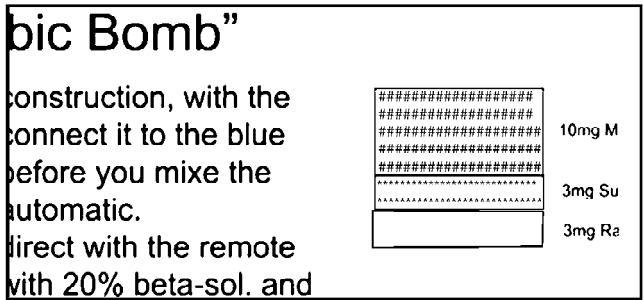


Fig. Instructions How to Build Weapons and Explosives are Available in Large Scale on the Internet. The Graphic Shows Explanations how to Build a Bomb by Only Using Components that are Available in Pharmacies.

Criminals can also use search engines to analyse targets. A training manual was found during investigations against members of a terrorist group highlighting how useful the Internet is for gathering information on possible targets.

Using search engines, offenders can collect publicly available information (e.g., construction plans from public buildings) that help in their preparations.

It has been reported that insurgents attacking British troops in Afghanistan used satellite images from Google Earth.

Missing Mechanisms of Control

All mass communication networks - from phone networks used for voice phonecalls to the Internet - need central administration and technical standards to ensure operability. The ongoing discussions about Internet governance suggest that the Internet is no different compared with national and

even transnational communication infrastructure. The Internet also needs to be governed by laws and law-makers and law enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

The Internet was originally designed as a military network based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when components of the network were attacked.

As a result, the Internet's network infrastructure is resistant to external attempts at control. It was not originally designed to facilitate criminal investigations or to prevent attacks from inside the network.

Today, the Internet is increasingly used for civil services. With the shift from military to civil services, the nature of demand for control instruments has changed. Since the network is based on protocols designed from military purposes, these central control instruments do not exist and it is difficult to implement them retrospectively, without significant redesign of the network.

The absence of control instruments makes cyber crime investigations very difficult. One example of the problems posed by the absence of control instruments is the ability of users to circumvent filter technology using encrypted anonymous communication services. If access providers block certain websites with illegal content (such as child pornography), customers are generally unable to access those websites.

But the blocking of illegal content can be avoided, if customers use an anonymous communication server encrypting communications between them and the central server. In this case, providers may be unable to block requests because requests sent as encrypted messages cannot be opened by access providers.

Cybercrime: An Introduction

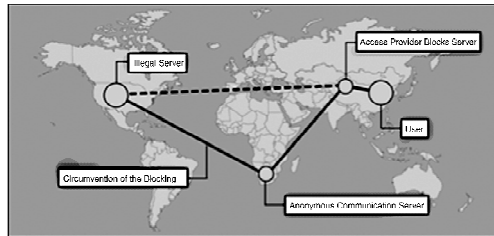


Fig. The Graphic Shows the Possibility of Circumventing Central Control Mechanisms Installed by Access Providers. If Access Providers Install Certain Filter Technology, User Requests will be Blocked. This Control Approach can be Circumvented, if the User makes Use of Anonymous Communication Servers that Encrypt Requests. For Example in this Case, Access Providers have no Access to Requests Sent to the Anonymous Communication Server and Cannot Block the Websites.

International Dimensions

Many data transfer processes affect more than one country. The protocols used for Internet data transfers are based on optimal routing if direct links are temporarily blocked. Even where domestic transfer processes within the source country are limited, data can leave the country, be transmitted over routers outside the territory and be redirected back into the country to its final destination.

Further, many Internet services are based on services from abroad *e.g.*, host providers may offer webspace for rent in one country based on hardware in another. If offenders and targets are located in different countries, cyber crime investigations need the cooperation of law enforcement agencies in all countries affected. National sovereignty does not permit investigations within the territory of different countries without the permission of local authorities. Cyber crime investigations need the support and involvement of authorities in all countries involved. It is difficult to base cooperation in cyber crime on principles of traditional mutual legal assistance. The formal requirements and time needed to collaborate with foreign law

enforcement agencies often hinder investigations. Investigations often occur in very short timeframes. Data vital for tracing offences are often deleted after only a short time. This short investigation period is problematic, because traditional mutual legal assistance regime often takes time to organise. The principle of dual criminality also poses difficulties, if the offence is not criminalised in one of the countries involved in the investigation. Offenders may be deliberately including third countries in their attacks to make investigation more difficult. Criminals may deliberately choose targets outside their own country and acting from countries with inadequate cyber crime legislation. The harmonisation of cyber crime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cyber crime investigations are the G8 24/7 Network and the provisions related to international cooperation in the Council of Europe Convention on Cyber crime.

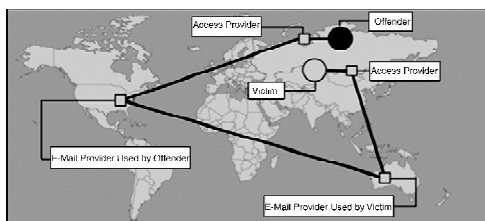


Fig. The Graphic Shows that, even if Offenders and Targets are Based in the Same Country, the act of Sending an e-mail with Illegal Content can Involve and Cross Various Countries. Even if this is not the Case, Data Transfer Processes may be Directed Outside the Country, before being Redirected Back.

Independence of Location and Presence at the Crime Site

Criminals need not be present at the same location as the target. As the location of the criminal can be completely different from the crime site, many cyber-offences are transnational. International cyber crime offences take considerable effort and time. Cybercriminals seek to avoid countries with strong cyber crime legislation.

Cybercrime: An Introduction

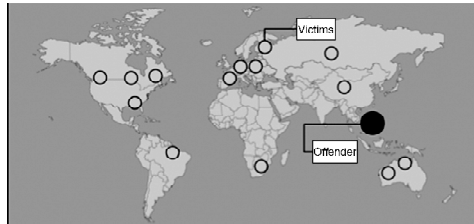


Fig. Offenders can Access the Internet to Commit Offences from Almost Anywhere in the World. Issues that Potential Offenders Take into Account while Deciding where to base Themselves Include: the Status of Cyber crime Legislation, the Effectiveness of Law Enforcement Agencies and the Availability of Anonymous Internet Access.

Preventing “safe havens” is one of the key challenges in the fight against cyber crime. While “safe havens” exist, offenders will use them to hamper investigation. Developing countries that have not yet implemented cyber crime legislation may become vulnerable, as criminals may choose to base themselves in these countries to avoid prosecution. Serious offences affecting victims all over the world may be difficult to stop, due to insufficient legislation in the country where offenders are located. This may lead to pressure on specific countries to pass legislation. One example of this is the “Love Bug” computer worm developed by a suspect in the Philippines in 2000, which infected millions of computers worldwide. Local investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalised in the Philippines. Another example is Nigeria, which has come under pressure to take action over financial scams distributed by e-mail.

Automation

One of the greatest advantages of ICTs is the ability to automate certain processes.

Automation has several major consequences:

- It increases the speed of processes;
- It increases the scale and impact of processes;
- It limits the involvement of humans.

Automation reduces the need for cost-intensive

manpower, allowing providers to offer services at lower prices. Offenders can use automation to scale up their activities - many millions of unsolicited bulk spam messages can be sent out by automation.

Hacking attacks are often also now automated, with as many as 80 million hacking attacks every day due to the use of software tools that can attack thousands of computer systems in hours. By automating processes offenders can gain great profit by designing scams that are based on a high number of offences with a relatively low loss for each victim. The lower the single loss is the higher is the chance that the victim will not report the offence.

```
PETRO VOICE HOLDING
Hot Stock in Momentum play for week

OTC: PHVC
This company is nasdaq bound

Petro Voice in on a roll earning Contrac

This is not a Fly by Night
Real market Cap, Real Earnings

View more on the latest news on PHVC
```

Fig. One Example for Automation Processes is the Dissemination of Spam. Millions of E-mails can be sent out within a Short Period of Time.

Automation of attacks affects developing countries in particular. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialised countries. The greater numbers of crimes that can be committed through automation pose challenges for law enforcement agencies worldwide, as they will have to be prepared for many more victims within their jurisdictions.

Resources

Modern computer systems that are now coming onto the market are powerful and can be used to extend criminal activities. But it is not just increasing power of single-user computers that poses problems for investigations. Increasing

network capacities is also a major issue. One example is the recent attacks against government websites in Estonia. Analysis of the attacks suggests that they were committed by thousands of computers within a “botnet” or group of compromised computers running Programmes under external control. In most cases, computers are infected with malicious software that installs tools allowing perpetrators to take control. Botnets are used to gather information about targets or for high-level attacks.

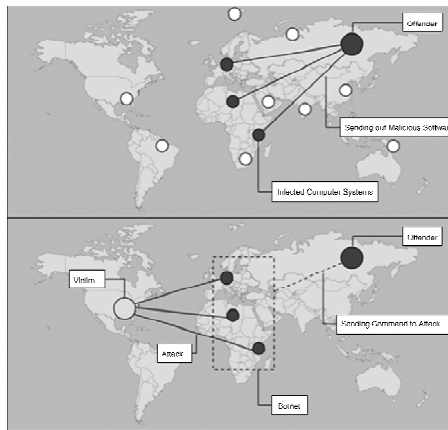


Fig.

Over recent years, botnets have become a serious risk for cyber security. The size of a botnet can vary, from a few computers to more than a million computers. Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet.

Botnets can be used for various criminal activities, including:

- Denial of Service attacks;
- Sending out spam;
- Hacking attacks;
- File-sharing networks.

Botnets offer a number of advantages for offenders. They increase both the computer and network capacity of criminals.

Using thousands of computer systems, criminals can attack computer systems that would be out of reach with only a few computers to lead the attack.

Botnets also make it more difficult to trace the original offender, as the initial traces only lead to the member of the botnets.

As criminals control more powerful computer systems and networks, the gap between the capacities of investigating authorities and those under control of criminals is getting wider.

Speed of Data Exchange Processes

The transfer of an e-mail between countries takes only a few seconds. This short period of time is one reason for the success of the Internet, as e-mails have eliminated the time for the physical transport of a message.

However, this rapid transfer leaves little time for law enforcement agencies to investigate or collect evidence. Traditional investigations take much longer. One example is the exchange of child pornography. In the past, pornographic videos were handed over or transported to buyers.

Both the handover and transport gave law enforcement agencies the opportunity to investigate. The main difference between the exchange of child pornography on and off the Internet is transportation. When offenders use the Internet, movies can be exchanged in seconds.

E-mails also demonstrate the importance of immediate response tools that can be used immediately. For tracing and identifying suspects, investigators often need access to data that may be deleted shortly after transfer. A very short response time by the investigative authorities is often vital for a successful investigation.

Without adequate legislation and instruments allowing investigators to act immediately and prevent data from being deleted, an effective fight against cyber crime may not be possible.

Cybercrime: An Introduction

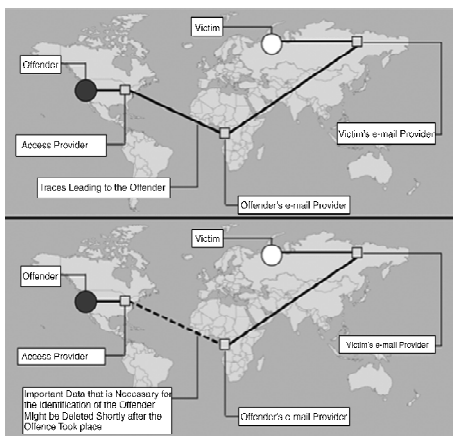


Fig. The Graphic Shows the Importance of Immediate Response in Cyber crime Investigations. Important Data that are Generated During the Process of Sending out an e-mail and that can Enable the Identification of the Offender are often Deleted Short after the e-mail was Send out. Without Access to this Information, Identification of the Offender is often Impossible.

“Quick freeze procedures” and 24/7 network points are examples for tools that can speed up investigations. Data retention legislation also aims to increase the time available for law enforcement agencies to carry out investigations. If the data necessary to trace offenders are preserved for a length of time, law enforcement agencies have a better chance of identifying suspects successfully.

Speed of Development

The Internet is constantly undergoing development. The creation of a graphical user interface (WWW) marked the start of its dramatic expansion, as previous command-based services were less user-friendly. The creation of the WWW has enabled new applications, as well as new crimes - law enforcement agencies are struggling to keep up.

Further developments continue, notably with:

- Online games;
- Voice over IP (VoIP) communications.

Online games are ever more popular, but it is unclear whether law enforcement agencies can successfully investigate and prosecute offences committed in this virtual world. The switch from traditional voice calls to Internet telephony also presents new challenges for law enforcement agencies. The techniques and routines developed by law enforcement agencies to intercept classic phone calls do not generally apply to VoIP communications. The interception of traditional voice calls is usually carried out through telecom providers. Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners.

Therefore, new techniques are needed. New hardware devices with network technology are also developing rapidly. The latest home entertainment systems turn TVs into Internet Access Points, while more recent mobile handsets store data and connect to the Internet via wireless networks.

USB (Universal Serial Bus) memory devices with more than 1 GB capacity have been integrated into watches, pens and pocket knives. Law enforcement agencies need to take these developments into account in their work - it is essential to educate officers involved in cyber crime investigations continuously, so they are up to date with the latest technology and able to identify relevant hardware and any specific devices that need to be seized. Another challenge is the use of wireless access points. The expansion of wireless Internet access in developing countries is an opportunity, as well as a challenge for law enforcement agencies. If offenders use wireless access points that do not require registration, it is more challenging for law enforcement agencies to trace offenders, as investigations lead only to access points.

Anonymous Communications

Certain Internet services make it difficult to identify offenders. The possibility of anonymous communication is

either just a by-product of a service or offered with the intention to avoid disadvantages for the user.

Examples for such services – that can even be combined are:

- Public Internet terminals (e.g., at airport terminals or Internet cafés);
- Wireless networks;
- Prepaid mobile services that do not need registration;
- Storage capacities for homepages offered without registration;
- Anonymous communication servers;
- Anonymous remailers.

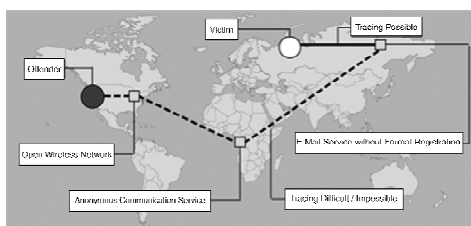


Fig. The Graphic Illustrates how Offenders can Achieve Anonymity by Combining Different Approaches. The Use of Open Wireless Networks makes it Almost Impossible to Identify Offenders. By Using Anonymous Communication Services and e-mail Services that do not verify Registration Information, Offender can reduce the chances of Successful Identification.



Fig. The Graphic Shows how Information can be Hidden in a Picture. The Encryption Software Includes Information by Altering the Information of Certain Pixels. If the Picture is Sufficiently Large, Changes can Hardly be Recognised without Having Access to the Original, as well as the Modified, Picture. Using this Technology, Offenders Can Hide the Fact that they are Exchanging Additional Information.

Offenders can hide their identities through, for example, the use of fake e-mail addresses. Many providers offer free e-mail addresses. Where personal information should be entered, it may not be verified, so users can register e-mail addresses without revealing their identity. Anonymous e-mail addresses can be useful *e.g.*, if users wish to join political discussion groups without identification.

Anonymous communications may give rise to anti-social behaviour, but they can also allow users to act more freely. Taking into consideration the various traces the users leave clarifies the need to enable instruments to prevent the user from profiling activities. Therefore various states and organisations support the principle of anonymous use of Internet e-mail services *e.g.*, this principle is expressed in the European Union Directive on Privacy and Electronic Communications.

One example of a legal approach to protect user privacy can be found in Article 37 of the European Union Regulation on Data Protection. However, some countries are addressing the challenges of anonymous communications by implementing legal restrictions – one example is Italy, which requires public Internet access providers to identify users, before they start using the service. These measures aim to help law enforcement agencies identify suspects, but they can be easily avoided - criminals may use unprotected private wireless networks or SIM-cards from countries not requiring registration. It is unclear whether the restriction of anonymous communications and anonymous access to the Internet should play a more important role in cyber security strategies.

Encryption Technology

Another factor that can complicate the investigation of cyber crime is encryption technology, which protects information from access by unauthorised people and is a key technical solution in the fight against cyber crime. Like anonymity, encryption is not new, but computer technology has transformed the field. It is now possible to encrypt computer data with the click of a mouse, making it difficult

for law enforcement agencies to break the encryption and access the data. It is uncertain to what extent offenders already use encryption technology to mask their activities – for example, it has been reported that terrorists are using encryption technology. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology but experts highlight the threat for an increasing use of encryption technology in Cyber crime cases.

Tools are available to break encryption. Various software products are available enabling users to protect files against unauthorised access. It is possible, but often difficult and slow, to break encryption – if investigators have access to the software used to encrypt files, they may be able to unpick the encryption. Alternatively, they may be able to break the encryption through, for example, a brute force attack. Depending on encryption technique and key size, it could take decades to break an encryption.

For example, if an offender uses encryption software with a 20-bit encryption, the size of the keyspace is around one million. Using a current computer processing one million operations per second, the encryption could be broken in less than one second. However, if offenders use a 40-bit encryption, it could take up to two weeks to break the encryption. Using a 56-bit encryption, a single computer would take up to 2,285 years to break the encryption.

If offenders use a 128-bit encryption, a billion computer systems operating solely on the encryption could take thousands of billion years to break it. The latest version of the popular encryption software PGP permits 1024-bit encryption. Current encryption software goes far beyond the encryption of single files. The latest version of Microsoft's operating Systems, for example, allows the encryption of an entire hard disk. Users can easily install encryption software. Although some computer forensic experts believe that this function does not threaten them, the widespread availability of this technology for any user could result in greater use of encryption. Tools are also available to encrypt communications

– for example, e-mails and phone calls can be sent using VoIP. Using encrypted VoIP technology, offenders can protect voice conversations from interception. Techniques can also be combined. Using software tools, offenders can encrypt messages and exchange them in pictures or images – this technology is called steganography. For investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages.

The availability and use of encryption technologies by criminals is a challenge for law enforcement agencies. Various legal approaches to address the problem are currently under discussion, including: potential obligations for software developers to install a back-door for law enforcement agencies; limitations on key strength; and obligations to disclose keys, in the case of criminal investigations. But encryption technology is not only used by offenders – there are various ways such technology is used for legal purposes. Without adequate access to encryption technology, it may be difficult to protect sensitive information. Given the growing number of attacks, self-protection is an important element of cyber security.

LEGAL CHALLENGES

Challenges in Drafting National Criminal Laws

Proper legislation is the foundation for the investigation and prosecution of cyber crime. However, law-makers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.

Historically, the introduction of computer-related services or Internet-related technologies gave rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s – the first unauthorised access to computer networks occurred shortly afterwards. Similarly, the first software offences appeared soon after the introduction of personal computers

in the 1980s, when these systems were used to copy software products. It takes time to update national criminal law to prosecute new forms of online cyber crime – some countries have not yet finished with this adjustment process. Offences that have been criminalised under national criminal law need to be reviewed and updated – for example, digital information must have equivalent status as traditional signatures and printouts.

Without the integration of cyber crime-related offences, violations cannot be prosecuted. The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law. This challenge remains as relevant and topical as ever as the speed of network innovation accelerates. Many countries are working hard to catch up with legislative adjustments.

In general, the adjustment process has three steps: Adjustments to national law must start with the recognition of an abuse of new technology. Specific departments are needed within national law enforcement agencies, which are qualified to investigate potential cyber crimes. The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

The second step is the identification of gaps in the penal code. To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences. In many cases, existing laws may be able to cover new varieties of existing crimes (*e.g.*, laws addressing forgery may just as easily be applied to electronic documents). The need for legislative amendments is limited to those offences that are omitted or insufficiently covered by the national law. The third step is the drafting of new legislation. Based on experience, it may be difficult for national authorities to execute the drafting process for cyber crime without international cooperation, due to the rapid development of

network technologies and their complex structures. Drafting cyber crime legislation separately may result in significant duplication and waste of resources and it is also necessary to monitor the development of international standards and strategies. Without the international harmonisation of national criminal legal provisions, the fight against trans-national cyber crime will run into serious difficulties due to inconsistent or incompatible national legislations. Consequently, international attempts to harmonise different national penal laws are increasingly important. National law can greatly benefit from the experience of other countries and international expert legal advice.

New Offences

In most cases, crimes committed using ICTs are not new crimes, but scams modified to be committed online. One example is fraud – there is not much difference between someone sending a letter with the intention to mislead another person and an e-mail with the same intention. If fraud is already a criminal offence, adjustment of national law may not be necessary to prosecute such acts. The situation is different, if the acts performed are no longer addressed by existing laws.

In the past, some countries had adequate provisions for regular fraud, but were unable to deal with offences where a computer system was influenced, rather than a human. For these countries, it has been necessary to adopt new laws criminalising computer-related fraud, in addition to the regular fraud. Various examples show how the extensive interpretation of existing provisions cannot substitute for the adoption of new laws.

Apart from adjustment for well-known scams, law-makers must continuously analyse new and developing types of cyber crime to ensure their effective criminalisation. One example of a cyber crime that has not yet been criminalised in all countries is theft and fraud in computer and online games. For a long time, discussions about online games focused on youth protection issues (*e.g.*, the requirement for verification of age) and illegal content (*e.g.*, access to child pornography in

the Online game "Second Life"). New criminal activities are constantly being discovered – virtual currencies in online games may be "stolen" and traded in auction platforms. Some virtual currencies have a value in terms of real currency (based on an exchange rate), giving the crime a 'real' dimension. Such offences may not be prosecutable in all countries. In order to prevent safe havens for offenders, it is vital to monitor developments worldwide.

Increasing Use of ICTs and the Need for New Investigative Instruments

Offenders use ICTs in various ways in the preparation and execution of their offences. Law enforcement agencies need adequate instruments to investigate potential criminal acts. Some instruments (such as data retention) could interfere with the rights of innocent Internet users. If the severity of the criminal offence is out of proportion with the intensity of interference, the use of investigative instruments could be unjustified or unlawful. As a result, some instruments that could improve investigation have not yet been introduced in a number of countries. The introduction of investigative instruments is always the result of a trade-off between the advantages for law enforcement agencies and interference with the rights of innocent Internet users. It is essential to monitor ongoing criminal activities to evaluate whether threat levels change. Often, the introduction of new instruments has been justified on the basis of the "fight against terrorism", but this is more of a far-reaching motivation, rather than a specific justification *per se*.

Developing Procedures for Digital Evidence

Especially due the low costs compared to the storage of physical documents, the number of digital documents is increasing. The digitalisation and emerging use of ICT has a great impact of procedures related to the collection of evidence and its use in court. As a consequence of the development digital evidence was introduced as a new source of evidence. It is defined as any data stored or transmitted using computer

technology that supports the theory of how an offence occurred. Handling digital evidence is accompanied with unique challenges and requires specific procedures. One of the most difficult aspects is to maintain the integrity of the digital evidence.

Digital data is highly fragile and can easily be deleted or modified. This is especially relevant for information stored in the system memory RAM that is automatically deleted when the system is shut down and therefore requires special preservation techniques.

In addition, new developments can have great impact on dealing with digital evidence. An example is cloud-computing. In the past investigators were able to focus on the suspects premise while searching for computer data. Today they need to take into consideration that digital information might be stored abroad and can only be accessed remotely, if necessary. Digital evidence plays an important role in various phases of cyber crime investigations.

It is in general possible to separate between four phases:

1. Identification of the relevant evidence;
2. Collection and preservation of the evidence;
3. Analysis of computer technology and digital evidence;
4. Presentation of the evidence in court.

In addition to the procedures that relate to the presentation of digital evidence in court, the ways in which digital evidence is collected requires special attention.

The collection of digital evidence is linked to computer forensics. The term 'computer forensics' describes the systematic analysis of IT equipment with the purpose of searching for digital evidence.

With regard to the fact that the amount of data stored in digital format constantly increases, highlights the logistic challenges of such investigations. Approaches to automated forensic procedures by, for example, using hash-value based searches for known child pornography images or a keyword search therefore play an important role in addition to manual investigations.

Depending on the requirement of the specific investigation, computer forensics could for example include the following:

- Analysing the hardware and software used by a suspect;
- Supporting investigators in identifying relevant evidence;
- Recovering deleted files;
- Decrypting files;
- Identifying Internet users by analysing traffic data.

Chapter 8

Anti-Cyber Crime Strategies

The growing number of recognised cyber crimes and technical tools to automate cyber crime offences mean that the fight against cyber crime has become an essential element of law enforcement activities worldwide. Cyber crime is a challenge to law enforcement agencies in both developed and developing countries. Since ICTs develop so rapidly, especially in developing countries, the creation and implementation of an effective anti-cyber crime strategy as part of a national cyber security strategy is essential.

CYBER CRIME LEGISLATION AS AN INTEGRAL PART OF A CYBER SECURITY STRATEGY

Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cyber crime – can help to reduce the risk of cyber crime.

An Anti-Cyber crime Strategy should be an integral element of a Cyber security Strategy. The ITU Global Cyber security Agenda, as a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cyber security and to enhance confidence and security in the information society, builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address these related

challenges. All the required measures highlighted in the five pillars of Global Cyber security Agenda are relevant to any cyber security strategy. Furthermore, the ability to effectively fight against cyber crime requires measures to be undertaken within all of the five pillars.

IMPLEMENTATION OF EXISTING STRATEGIES

One possibility is that anti-cyber crime strategies developed in industrialised countries could be introduced in developing countries, offering advantages of reduced cost and time for development. The implementation of existing strategies could enable developing countries to benefit from existing insights and experience. Nevertheless, the implementation of an existing anti-cyber crime strategy poses a number of difficulties. Although similar challenges confront both developing and developed countries, the optimal solutions that might be adopted depend on the resources and capabilities of each country. Industrialised countries may be able to promote cyber security in different and more flexible ways – *e.g.*, by focusing on more cost-intensive technical protection issues.

There are several other issues that need to be taken into account by developing countries adopting existing anticypber crime strategies:

- Compatibility of respective legal systems;
- Status of supporting initiatives (*e.g.* education of the society);
- Extent of self-protection measures in place;
- Extent of private sector support (*e.g.*, through Public-Private Partnerships), among other issues.

REGIONAL DIFFERENCES

Given the international nature of cyber crime, the harmonisation of national laws and techniques is vital in the fight against cyber crime. However, harmonisation must take into account regional demand and capacity. The importance of regional aspects in the implementation of anti-cyber crime strategies is underlined by the fact that many legal and

technical standards were agreed among industrialised countries and do not include various aspects important for developing countries. Therefore, regional factors and differences need to be included within their implementation elsewhere.

RELEVANCE OF CYBER CRIME ISSUES WITHIN THE PILLARS OF CYBER SECURITY

The Global Cyber security Agenda has seven main strategic goals, built on five work areas:

1. Legal Measures;
2. Technical and Procedural Measures;
3. Organizational Structures;
4. Capacity Building;
5. International Cooperation.

Issues related to cyber crime play an important role in all five pillars of the Global Cyber security Agenda. Among these work areas, the Legal Measures work areas focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.

Legal Measures

Within the five pillars the legal measure are probably the most relevant with regard to an Anti-Cyber crime Strategy. This requires first of all the necessary substantive criminal law provisions to criminalise acts such as computer fraud, illegal access, data interference, copyright violations and child pornography. The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.

Therefore, a thorough analysis of current national laws is vital to identify any possible gaps. Apart from substantive criminal law provisions, the law enforcement agencies need the necessary tools and instruments to investigate cyber crime. Such investigations themselves present a number of challenges. Perpetrators can act from nearly any location in the world and take measures to mask their identity. The tools and instruments

needed to investigate cyber crime can be quite different from those used to investigate ordinary crimes. Due to the international dimension of cyber crime it is in addition necessary to develop the legal national framework to be able to cooperate with law enforcement agencies abroad.

Technical and Procedural Measures

Cyber crime-related investigations very often have a strong technical component. In addition the requirement of maintaining the integrity of the evidence during an investigation requires precise procedures. The development of the necessary capacities as well as procedures is therefore a necessary requirement related to fight against cyber crime. Another issue is the development of technical protection systems.

Well-protected computer systems are more difficult to attack. Improving technical protection by implementing proper security standards is an important first step. For example, changes in the online banking system (*e.g.*, the switch from TAN to ITAN) have eliminated much of the danger posed by current “phishing” attacks, demonstrating the vital importance of technical solutions. Technical protection measures should include all elements of the technical infrastructure – the core network infrastructure, as well as the many individually connected computers worldwide.

Two potential target groups can be identified for protecting Internet users and businesses:

1. End users and businesses (direct approach); and
2. Service providers and software companies.

Logistically, it can be easier to focus on protection of core infrastructure (*e.g.*, backbone network, routers, essential services), rather than integrating millions of users into an Anti-Cyber crime Strategy. User protection can be achieved indirectly, by securing the services consumers use – *e.g.*, online banking. This indirect approach to protecting Internet users can reduce the number of people and institutions that need to be included in steps to promote technical protection. Although limiting the number of people that need to be included in

technical protection might seem desirable, computer and Internet users are often the weakest link and the main target of criminals. It is often easier to attack private computers to obtain sensitive information, rather than the well-protected computer systems of a financial institution.

Despite these logistical problems, the protection of end-user infrastructure is vital for the technical protection of the whole network. Internet Service Providers and product vendors (e.g. software companies) play a vital role in the support of anticyber crime strategies. Due to their direct contact with clients, they can operate as a guarantor of security activities (e.g., the distribution of protection tools and information on the current status of most recent scams).

Organizational Structure

An effective fight against cyber crime requires highly developed organizational structures. Without having the right structures in place that avoids overlapping and is based on clear competences it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts.

Capacity Building and User Education

Cyber crime is a global phenomenon. In order to be able to effectively investigate offences harmonisation of laws and the development of means of international cooperation needs to be established. In order to ensure global standards in developed countries as well as in developing countries capacity building is necessary.

In addition to capacity building user education is required. Certain cyber crimes – especially those related to fraud, such as “phishing” and “spoofing” – do not generally depend on a lack of technical protection, but rather lack of awareness by victims. There are various software products that can automatically identify fraudulent websites, but until now, these products cannot identify all suspicious websites. A user protection strategy based only on software products has limited ability to protect the users. Although the technical protection

measures continue to develop and the products available are updated on a regular basis, such products cannot yet substitute for other approaches. One of the most important elements in the prevention of cyber crime is user education. For example, if users are aware that their financial institutions will never contact them by e-mail requesting passwords or bank account details, they cannot fall victim to phishing or identity fraud attacks. The education of Internet users reduces the number of potential targets.

Users can be educated through:

- Public campaigns;
- Lessons in schools, libraries, IT centres and universities;
- Public Private Partnerships (PPPs).

One important requirement of an efficient education and information strategy is the open communication of the latest cyber crime threats. Some states and/or private businesses refuse to emphasize that citizens and clients respectively are affected by cyber crime threats, in order to avoid them losing trust in online communication services. The United States Federal Bureau of Investigation has explicitly asked companies to overcome their aversion to negative publicity and report cyber crime. In order to determine threat levels, as well as to inform users, it is vital to improve the collection and publication of relevant information.

International Cooperation

In a large number of cases data transfer processes in the Internet affect more than one country. This is a result of the design of the network as well as the fact the protocols that ensures that successful transmissions can be made, even if direct lines are temporarily blocked.

In addition a large number of Internet services (like for example hosting services) are offered by companies that are based abroad. In those cases where the offender is not based in the same country at the victim, the investigation requires cooperation between law enforcement agencies in all countries that affected. International and transnational investigations

without the consent of the competent authorities in the countries involved are difficult with regards to the principle of National Sovereignty. This principle does in general not allow one country to carry out investigations within the territory of another country without the permission of the local authorities. Therefore, investigations need to be carried out with the support of the authorities in all countries involved. With regard to the fact that in most cases there is only a very short time gap available in which successful investigations can take place, the application of the classic mutual legal assistance regimes involves clear difficulties when it comes to cyber crime investigations. This is due to the fact that mutual legal assistance in general requires time consuming formal procedures. As a result improvement in terms of enhanced international cooperation plays an important and critical role in the development and implementation of cyber security strategies and anti-cyber crime strategies.

Chapter 9

International Legislative Approaches

INTERNATIONAL APPROACHES

A number of international organisations work constantly to analyse the latest developments in cyber crime and have set up working groups to develop strategies to fight these crimes.

The G8

In 1997, the Group of Eight (G8) established a “Subcommittee on High-tech Crimes” dealing with the fight against cyber crime. During their meeting in Washington D.C., United States, the G8 Justice and Interior Ministers adopted Ten Principles and a Ten-Point Action Plan to fight high-tech crimes.

The Heads of the G8 endorsed these principles later, which include:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
- Law enforcement personnel must be trained and equipped to address high-tech crimes.

In 1999, the G8 specified their plans regarding the fight against high-tech crimes at a Ministerial Conference on Combating Transnational Organised Crimes in Moscow, Russian Federation. They expressed their concerns about

crimes (such as child pornography), as well as traceability of transactions and transborder access to stored data. Their Communiqué contains a number of principles in the fight against cyber crime that are today found in a number of international strategies.

One of the practical achievements of the work done by expert groups has been the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week. At the G8 Conference in Paris, France in 2000, the G8 addressed the topic of cyber crime with a call to prevent lawless digital havens.

Already at that time, the G8 connected its attempts for international solutions to the Council of Europe's Convention on Cyber crime. In 2001, the G8 discussed procedural instruments in the fight against cyber crime at a workshop held in Tokyo, focusing on whether data retention obligations should be implemented or whether data preservation was an alternative solution. In 2004, the G8 Justice and Home Affairs Ministers issued a Communiqué in which they addressed the need for the creation of global capacities in the fight against criminal uses of the Internet.

Again, the G8 took note of the Council of Europe's Convention on Cyber crime. During the 2006 Moscow Meeting, the G8 Justice and Home Affairs Ministers discussions issues related to the fight Cyber crime and the issues of cyberspace and especially the necessity of improving effective countermeasures.

The meeting of the G8 Justice and Home Affairs Ministers was followed by the G8 Summit in Moscow where the issue of Cyber terrorism was discussed.

During the 2007 meeting the of the G8 Justice and Interior Ministers in Munich, Germany the issue of terrorist use of the Internet was further discussed and the participants agreed to criminalise the misuse of the Internet by terrorist groups. This agreement did not include specific acts that the states should criminalise.

At the 8th Congress on the Prevention of Crime and the Treatment of Offenders, the UN General Assembly adopted a resolution dealing with computer crime legislation. Based on its Resolution 45/121, the UN published a manual in 1994 on the prevention and control of computer-related crime. In 2000, the General Assembly adopted a Resolution on combating the criminal misuse of information technologies that shows a number of similarities with the Ten-Point Action Plan by the G8 from 1997.

In its Resolution, the General Assembly identified a number of measures to prevent the misuse of information technology, including:

- States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;
- Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;
- Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies.

In 2002, the General Assembly adopted another Resolution on combating the criminal misuse of information technology.

The Resolution refers to the existing international approaches in fighting cyber crime and highlights various solutions.

- Noting the work of international and regional organizations in combating high- technology crime, including the work of the Council of Europe in elaborating the Convention on Cyber crime as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,
- Invites Member States, when developing national law, policy and practice to combat the criminal misuse of

information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

- Takes note of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;
- Decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice.

In 2004, the UN created a working group dealing with spam, cyber crime and other Internet-related topics, emphasising the interest of the UN in participating in ongoing international discussions on cyber crime threats. At the 11th UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand in 2005, a Declaration was adopted that highlighted the need for harmonisation in the fight against cyber crime.

Among them the following issues:

- We reaffirm the fundamental importance of implementation of existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures, in particular against cyber crime, moneylaundering and trafficking in cultural property, as well as on extradition, mutual legal assistance and the confiscation, recovery and return of proceeds of crime.
- We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those

technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent investigate and prosecute high-technology and computer-related crime, including by developing partnerships with the private sector. We recognise the important contribution of the United Nations to regional and other international forums in the fight against cyber crime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

In addition, a number of United Nations system Decisions, Resolutions and Recommendations address issues related to cyber crime.

The most important ones are:

- The United Nations Office for Drugs and Crime (UNODC) Commission on Crime Prevention and Criminal Justice adopted a Resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.
- In 2004 the United Nations Economic and Social Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes. In 2007 the Council adopted a resolution on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identityrelated crime. Both resolutions do not explicitly address the challenges of Internet-related crimes but is applicable with regard to those offences as well.

In 2004 the Council adopted a resolution on the sale of licit drugs via the Internet that was explicitly taking regard to a phenomenon related to a computer crime.

The International Telecommunication Union (ITU), as a specialised agency within the United Nations, plays a leading role in the standardization and development of telecommunications as well as cyber security issues. Among other activities, the ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases in Geneva, Switzerland and in Tunis, Tunisia. Governments, policymakers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with the development of a global information society, including the development of compatible standards and laws.

The outputs of the Summit are contained in the Geneva Declaration of Principles, the Geneva Plan of Action; the Tunis Commitment and the Tunis Agenda for the Information Society.

- The Geneva Plan of Action highlights the importance of measures in the fight against cyber crime: C5. Building confidence and security in the use of ICTs
- Confidence and security are among the main pillars of the Information Society.
- Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

Cyber crime was also addressed at the second phase of WSIS in Tunis in 2005.

The Tunis Agenda for the Information Society highlights the need for international cooperation in the fight against cyber crime and refers to the existing legislative approaches such as the UN General Assembly Resolutions and the Council of Europe Convention on Cyber crime:

- We underline the importance of the prosecution of cyber crime, including cyber crime committed in one jurisdiction, but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, *inter alia*, law-enforcement agencies on cyber crime. We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cyber crime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cyber crime.

As an outcome of the WSIS, ITU was nominated as the sole Facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology. At the second Facilitation Meeting for WSIS Action Line C5 in 2007, the ITU Secretary-General highlighted the importance of international cooperation in the fight against cyber crime and announced the launch of the *ITU Global Cyber security Agenda*. The Global Cyber security Agenda is made up of seven key goals, and built upon five strategic pillars, including the elaboration of strategies for the development of model cyber crime legislation.

The main goals are the following:

- Elaboration of strategies for the development of a model cyber crime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
- Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cyber crime.
- Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems.

- Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.
- Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.
- Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.
- Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

Council of Europe

In 1976, the Council of Europe (CoE) highlighted the international nature of computer-related crimes and discussed the topic at a conference dealing with aspects of economic crimes.

This topic has since remained on its agenda. In 1985, the Council of Europe appointed an Expert Committee to discuss the legal aspects of computer crimes.

In 1989, the European Committee on Crime Problems adopted the "Expert Report on Computer-Related Crime", analysing the substantive criminal legal provisions necessary to fight new forms of electronic crimes, including computer fraud and forgery.

The Committee of Ministers in 1989 adopted a Recommendation that specifically highlighted the international nature of computer crime:

- The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

- Recognising the importance of an adequate and quick response to the new challenge of computer-related crime; Considering that computer-related crime often has a transfrontier character; Aware of the resulting need for further harmonisation of the law and practice, and for improving international legal co-operation, Recommends the governments of member states to:
 - Take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime elaborated by the European Committee on Crime Problems, and in particular the guidelines for the national legislatures;
 - Report to the Secretary General of the Council of Europe during 1993 on any developments in their legislation, judicial practice and experiences of international legal co-operation in respect of computer-related crime.

In 1995, the Committee of Ministers adopted another recommendation dealing with the problems arising from transnational computer crimes. The European Committee on Crime Problems (CDPC) decided in 1996 to set up a Committee of experts to deal with cyber crime. The idea of going beyond principles for another recommendation and drafting a Convention was present at the time of the establishment of the Committee of Experts. Between 1997 and 2000, the Committee held ten meetings in plenary and fifteen meetings of its open-ended Drafting Group. The Assembly adopted the draft Convention at the 2nd part of its plenary session in April 2001. The finalised draft Convention was submitted for approval to the CDPC, and afterwards the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature. The Convention was opened for signature at a signing ceremony in Budapest on 23 November, 2001, during which 30 countries signed the Convention (including four non-members of the Council of Europe Canada, United States, Japan and South

Africa that participated in the negotiations). By April 2009, 46 States have signed and 25 States have ratified the Convention on Cyber crime.

Countries such as Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have already drafted parts of their legislation in accordance with the Convention. Although those countries have not yet signed the Convention, they are supporting the harmonisation and standardisation process intended by the drafters of the Convention. The Convention is today recognised as an important international instrument in the fight against Cyber crime and is supported by different international organisations.

The Convention was followed by the First Additional Protocol to the Convention on Cyber crime. During the negotiations on the text of the Convention it turned out that especially the criminalisation of racism and the distribution of xenophobic material was a controversial matter. Some countries that had a strong protection of the principle of freedom of expression expressed their concern, that if provisions are included in the Convention that violate freedom of expression they would be unable to sign the Convention. Therefore those issues were integrated into a separate protocol. By October 2008, 20 States have signed and 13 States have ratified the Additional Protocol.

Within its approach to improve the protection of minors against sexual exploitation the Council of Europe introduced a new Convention in 2007. On the first day the Convention on the protection of children opened for signature 23 States signed the Convention. One of the key aims of the Convention is the harmonisation of criminal law provisions that are aiming to protect children from sexual exploitation.

To achieve this aim the Convention contains a set of criminal law provisions. Apart from the criminalisation of the sexual abuse of children (Art. 18) the Convention contains a provision dealing with the exchange of child pornography (Art. 20) and the solicitation of children for sexual purposes (Art. 23).

In addition to the international organisations that are globally active, a number of international organisations that focus on specific regions have moved forward on activities that deal with issues related to cyber crime.

European Union

The European Union has only limited powers with regard to the legislation in the field of criminal law. It has the ability to harmonise the national criminal law only in special areas such as the protection of financial interests of the European Union and cyber crime. In 1999, the European Union launched the initiative "eEurope", by adopting the European Commission's Communication "eEurope – An Information Society for all". In 2000, the European Council adopted a comprehensive "eEurope Action Plan" and called for its implementation before the end of 2002. In 2001, the European Commission published a Communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime".

In this Communication, the Commission analysed and addressed the problem of cyber crime and pointed out the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks.

- Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society. Some recent examples of denial of service and

virus attacks have been reported to have caused extensive financial damage.

- There is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act, whilst fully respecting the fundamental rights of individuals.
- The Commission having participated in both the CoE and the G8 discussions, recognises the complexity and difficulties associated with procedural law issues. But effective co-operation within the EU to combat Cyber crime is an essential element of a safer Information Society and the establishment of an Area of Freedom, Security and Justice.
- The Commission will bring forward legislative proposals under the Title VI of the TEU:
 - [...] to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks. The Commission will also examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. Finally, the problem of illicit drugs on the Internet will also be examined.
 - The Commission will continue to play a full role in ensuring co-ordination between Member States in other international fora in which Cyber crime is being discussed such as the Council of Europe and G8. The Commission's initiatives at EU level will take full account of progress in other international fora, while seeking to achieve approximation within the EU.

In addition, the Commission published a Communication on “Network and Information Security” in 2001 that analysed the problems in network security and drafted a strategic outline for action in this area. Both these Commission Communications emphasised the need for approximation of substantive criminal law within the European Union – especially with regard to attacks against information systems. The harmonisation of the substantive criminal law within the European Union in the fight against cyber crime is recognised as a key element of all initiatives at the EU-level. Following this strategy the Commission in 2002 presented a proposal for a “Framework Decision on Attacks against Information Systems”. The Proposal by the Commission was partly modified and finally adopted by the Council. The Framework Decision takes note of the Council of Europe Convention on Cyber crime but concentrates on the harmonisation of substantive criminal law provisions that are designed to protect infrastructure elements.

Article 2 – Illegal access to information systems:

- Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.
- Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure, punishable by effective, proportional and dissuasive criminal penalties.

Article 3 – Illegal system interference:

- Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4 – Illegal data interference:

- Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

In 2005, the Court of Justice for the European Communities declared a Council Framework Decision on the Protection of the Environment through Criminal Law unlawful. With this decision, the Court clarified the distribution of powers between the first and third pillars regarding provisions of criminal law. It decided that the Framework Decision on the Protection of the Environment through criminal law, being indivisible, infringes Article 47 EU as it encroaches on the powers, which Article 175 EC confers on the Community.

In a Communication on the Court Decision⁸⁵⁷the Commission expressed:

- “From the point of view of subject matter, in addition to environmental protection the Court’s reasoning can therefore be applied to all Community policies and freedoms which involve binding legislation with which criminal penalties should be associated in order to ensure their effectiveness.”

The Commission stated that as a result of the Court’s Judgement a number of framework decisions dealing with criminal law are entirely or partly incorrect, since all or some of their provisions were adopted on the wrong legal basis. The Framework Decision on Attacks against Information Systems is explicitly mentioned in the amendment of the communication. Aspects of criminal procedural law – especially the harmonisation of the instruments necessary to investigate and prosecute cyber crime – were not integrated in the Framework Decision. However, in 2005, the Commission drafted a Proposal for a European Union Directive dealing with data retention. Just three months after the presentation to the European Parliament, the Council adopted the proposal.

The key element of the Directive is the duty of Internet Providers to store certain traffic data that is necessary for the identification of criminal offenders in cyberspace:

- Article 3 – Obligation to retain data:
 - 1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.
 - 2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

The fact that key information about any communication in the Internet will be covered by the Directive lead to intensive criticism from human rights organisations and could lead to a review of the Directive and its implementation by constitutional courts.

In 2007, the Commission published a communication towards a general policy on the fight against cyber crime. The communication summarises the current situation and emphasises the importance of the Council of

Europe Convention on Cyber crime as the predominant international instrument in the fight against cyber crime.

In addition, the communication points out the issues that the Commission will focus on with regard to its future activities. These include:

- Strengthening international cooperation in the fight against cyber crime;
- Better coordinated financial support for training activities;
- The organisation of a meeting of law enforcement experts;
- Strengthening the dialog with the industry;
- Monitoring of the evolving threats of cyber crime to evaluate the need for further legislation.

In 2008 the European Union started a discussion about a Draft Amendment of the Framework Decision on Combating Terrorism.

In the introduction to the draft amendment, the European Union highlights that the existing legal framework criminalises aiding or abetting and inciting but does not criminalise the dissemination of terrorist expertise through the Internet. With the amendment the European Union is aiming to take measures to close the gap and bring the legislation throughout the European Union closer to the Council of Europe Convention on the Prevention of Terrorism.

Article 3 – Offences linked to terrorist activities:

1. For the purposes of this Framework Decision:
 - (a) "Public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the acts listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;
 - (b) "Recruitment for terrorism" means to solicit another person to commit one of the acts listed in Article 1(1), or in Article 2(2);

- (c) "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.
2. Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following intentional acts:
 - (a) Public provocation to commit a terrorist offence;
 - (b) Recruitment for terrorism;
 - (c) Training for terrorism;
 - (d) Aggravated theft with a view to committing one of the acts listed in Article 1(1);
 - (e) Extortion with a view to the perpetration of one of the acts listed in Article 1(1);
 - (f) Drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).
 3. For to be necessary that a terrorist offence be actually committed.

Based on Article 3, paragraph 1 (c) of the Framework, the Member States are for example obliged to criminalise the publication of instructions on how to use explosives, knowing that this information is intended to be used for terrorist-related purposes. The need for evidence that the information is intended to be used for terrorist-related purposes very likely limits the application of the provision with regard to the majority of instructions on how to use weapons that are available online, as their publication does not directly link them to terrorist attacks. As most of the weapons and explosives can be used to commit "regular" crimes as well as terrorist-related offences (dual use), the information itself can hardly be used to prove that the person who published them had

knowledge about the way such information is used afterwards. Therefore the context of the publication (e.g. on a Web site operated by a terrorist organisation) needs to be taken into consideration.

Organisation for Economic Co-operation and Development

In 1983, the Organisation for Economic Co-operation and Development (OECD) initiated a study on the possibility of an international harmonisation of criminal law in order to address the problem of computer crime. In 1985, it published a report that analysed the current legislation and made proposals for the fight against cyber crime. It recommended a minimum list of offences that countries should consider criminalising, e.g. computer-related fraud, computer-related forgery, the alteration of computer Programmes and data, and the interception of the communications. In 1990 the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council.

The guidelines include among other aspects, the issues of sanctions:

- Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer Programmes. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national

penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime. National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.

After reviewing the guidelines in 1997, the ICCP created a second Expert Group in 2001 that updated the guidelines. In 2002 a new version of the guidelines "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" was adopted as a Recommendation of the OECD Council.

The guidelines contain nine complementary principles:

1. *Awareness:* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. *Responsibility:* All participants are responsible for the security of information systems and networks.
3. *Response:* Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. *Ethics:* Participants should respect the legitimate interests of others.
5. *Democracy:* The security of information systems and networks should be compatible with essential values of a democratic society.
6. *Risk assessment:* Participants should conduct risk assessments.
7. *Security design and implementation:* Participants should incorporate security as an essential element of information systems and networks.
8. *Security management:* Participants should adopt a comprehensive approach to security management.
9. *Reassessment:* Participants should review and reassess the security of information systems and networks, and

make appropriate modifications to security policies, practices, measures and procedures.

In 2005, the OECD published a report that analysed the impact of Spam on developing countries. The report showed that due to the more limited and more expensive resources, spam is a much more serious issue in developing countries than in western countries.

After receiving a request from the Strategic Planning Unit of the Executive Office of the Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of the Internet for terrorist purpose, in 2007 OECD published a report on the legislative treatment of "Cyberterror" in the domestic law of individual states.

ASIA-PACIFIC ECONOMIC COOPERATION

In 2002 the Asia-Pacific Economic Cooperation (APEC) Leaders released a "Statement on Fighting Terrorism and Promoting Growth" to enact comprehensive laws relating to cyber crime and develop national cyber crime investigating capabilities.

They committed to:

- Endeavour to enact a comprehensive set of laws relating to cyber security and Cyber crime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 and Convention on Cyber crime by October 2003.
- Identify national Cyber crime units and international high-technology assistance points of contact and create such capabilities to the extent they do not already exist, by October 2003.
- Establish institutions that exchange threat and vulnerability assessment (such as Computer Emergency Response Teams) by October 2003.

APEC leaders have called for closer cooperation by officials involved in the fight against cyber crime. In 2005, APEC

organised a Conference on Cyber crime Legislation. The primary objectives of the conference were to:

- Promote the development of comprehensive legal frameworks to combat Cyber crime and promote cyber security;
- Assist law enforcement authorities to respond to cutting-edge issues and the challenges raised by advances in technology;
- Promote cooperation between Cyber crime investigators across the region.

The APEC Telecommunications and Information Working Group actively participated in APECs approaches to increase cyber security. In 2002 it adopted the APEC Cyber security Strategy. The Working Group expressed their position regarding cyber crime legislation by referring to existing international approaches from the UN and the Council of Europe.

The Declaration of the 2008 meeting of the APEC Telecommunications and Information Ministers in Bangkok, Thailand highlighted the importance of continuation of the collaboration against cyber crime.

The Commonwealth

Taking into account the rising importance of Cyber crime the Law Ministers of the Commonwealth decided to order an Expert Group to develop a legal framework for combating Cyber crime on the basis of the Council of Europe Convention on Cyber crime. This approach to harmonise legislation within the Commonwealth and enable international cooperation was among other issues influence by the fact that without such approach it would require not less than 1272 bilateral treaties within the Commonwealth to deal with international cooperation in this matter.

The Expert Group presented their report and recommendations in March 2002. Later in 2002 the Draft Model Law on Computer and Computer Related Crime was presented. Due to the clear instruction as well as the recognition of the Convention on Cyber crime as international

standard by the expert group the model law is in line with the standards defined by the Convention on Cyber crime.

The Arab League and Gulf Cooperation Council

A number of countries in the Arabic region have already undertaken national measures and adopted approaches to combat cyber crime, or are in the process of drafting legislation. Examples of countries include: Pakistan, Egypt and the United Arab Emirates (UAE). The Gulf Cooperation Council (GCC) recommended at a conference in 2007 that the GCC countries is seek a joint approach that takes into consideration international standards.

Organisation of American States

Since, 1999 the Organisation of American States (OAS) has actively been addressing the issue of cyber crime within the region. Among others, the organisation has held a number of meetings within the mandate and scope of REMJA, the Ministers of Justice or Ministers or Attorneys General of the Americas. In 1999, REMJA recommended the establishment of an intergovernmental experts group on cyber crime.

The expert group was mandated to:

- Complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offence;
- Complete a diagnosis of national legislation, policies and practices regarding such activity;
- Identify national and international entities with relevant expertise; and
- Identify mechanisms of cooperation within the Inter-American system to combat cyber crime.

In 2000 the Ministers of Justice or Ministers or Attorneys General of the Americas addressed the topic of cyber crime and agreed on a number of recommendations. These recommendations were repeated at the 2003 meeting and included:

- To support consideration of the recommendations made by the Group of Governmental Experts at its

initial meeting as the REMJA contribution to the development of the Inter-American Strategy to Combat Threats to Cyber security, referred to in OAS General Assembly resolution AG/RES. 1939/XXXIII-O/03), and to ask the Group, through its Chair, to continue to support the preparation of the Strategy.

- That Member States, in the context of the expert group, review mechanisms to facilitate broad and efficient cooperation among themselves to combat cyber crime and study, when possible, the development of technical and legal capacity to join the 24/7 network established by the G8 to assist in cyber crime investigations.
- That Member States evaluate the advisability of implementing the principles of the Council of Europe Convention on Cyber crime; and consider the possibility of acceding to that convention. That Member States review and, if appropriate, update the structure and work of domestic bodies, or agencies in charge of enforcing the laws so as to adapt to the shifting nature of cyber crime, including by reviewing the relationship between agencies that combat cyber crime and those that provide traditional police or mutual legal assistance.

The Fourth Meeting of Ministers of Justice or Ministers or Attorneys General of the Americas recommended that, in the framework of the activities of the OAS working group to follow up on the REMJA recommendations.

The Group of Governmental Experts on cyber crime be reconvened and mandated to:

- Follow up on implementation of the recommendations prepared by that Group and adopted by REMJA-III, and;
- Consider the preparation of pertinent inter-American legal instruments and model legislation for the purpose of strengthening hemispheric cooperation in combating cyber-crime, considering standards relating

to privacy, the protection of information, procedural aspects, and crime prevention.

The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA) has held seven meetings to date. The most recent meetings were held in Washington D.C., United States in April 2006 and April 2008.

Among the recommendations arising from the 2006 meeting were the following:

- To continue to strengthen cooperation with the Council of Europe so that the OAS Member States can give consideration to applying the principles of the Council of Europe's Convention on Cyber-Crime and to adhering thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cyber crime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation Forum, the OECD, the G-8, the Commonwealth, and INTERPOL, in order for the OAS Member States to take advantage of progress in those forums; and
- That Member States establish specialised units to investigate cyber crime, and identify the authorities who will serve as the points of contact in this matter and expedite the exchange of information and obtaining of evidence. In addition, to foster cooperation in efforts to combat cyber crime among government authorities and Internet service providers and other private sector enterprises providing data transmission services.

These recommendations were re-iterated at the 2008 meeting and the meeting further noted:

- That, bearing in mind the recommendations adopted by the Group of Governmental Experts and by the previous REMJA meetings, the states consider applying the principles of the Council of Europe's Convention

on Cyber-Crime, acceding thereto, and adopting the legal and other measures required for its implementation. Similarly, to this end, that technical cooperation activities continue to be held under the auspices of the OAS General Secretariat, through the Secretariat for Legal Affairs, and the Council of Europe. Similarly, that efforts be continued to strengthen the exchange of information and cooperation with other international organizations and agencies in the area of cyber crime, so that the OAS member states may take advantage of progress in those forums.

- That the Secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and the Working Group on Cyber-Crime, continue developing the permanent coordination and cooperation actions to ensure the implementation of the Comprehensive Inter-American Cyber security Strategy adopted through OAS General Assembly resolution AG/RES. 2004.

SCIENTIFIC APPROACHES

A well known example of a scientific approach to developing a legal framework for addressing cyber crime at the global level is the Stanford Draft International Convention (CISAC). This Convention was developed as a follow up to a conference hosted by Stanford University in the United States in 1999. Comparing the Council of Europe Convention on Cyber crime that was drafted around the same time shows a number of similarities.

Both cover aspects of substantive criminal law, procedural law and international cooperation. The most important difference is the fact, that the offences and procedural instruments developed by the Stanford Draft Convention are only applicable with regard to attacks on information infrastructure and terrorist attacks while the instruments related to procedural law and international cooperation

mentioned in the Convention on Cyber crime can also be applied with regard to traditional offences as well.

THE RELATIONSHIP BETWEEN DIFFERENT INTERNATIONAL LEGISLATIVE APPROACHES

The success of single standards with regard to technical protocols leads to the question of how conflicts between different international approaches can be avoided. Currently the Convention on Cyber crime is the main international framework in place that covers all relevant aspect so cyber crime, but other initiatives are also being discussed. A second international approach is currently undertaken by the International Telecommunication Union.

Following the World Summit on the Information Society, the ITU was nominated as the facilitator for the so called WSIS Action Line C5. As defined at the Geneva phase of the WSIS Summit in 2003, Action Line C5 contains the building of confidence and security in the use of ICTs. At the second facilitation meeting for the follow up for Action Line C5, the ITU Secretary–General emphasised the importance of international cooperation in the fight against cyber crime.

This was followed by the announcement of the development of the ITU Global Cyber security Agenda. The ITU Global Cyber security Agenda (GCA) contains seven key goals. One of these goals is the elaboration of strategies for the development of model cyber crime legislation. An expert group was created to provide strategies related to the GCA. The answer to the question how a possible model law interacts with the existing standards depends on the approach taken in drafting a new model law.

In general there are three possible relations:

- *Controversial Regulations:* If a new model law defines standards that are not in accordance with the existing standards, this could, at least initially, have a negative effect on the necessary harmonisation process.
- *Partly Duplicating the Convention's Standards:* A new model law could be based on the Convention on Cyber crime and could eliminate those provisions that led

to difficulties or even stopped countries from signing the Convention. An example is the controversially discussed regulation in Art. 32b Convention on Cyber crime. This provision was criticised by the Russian Delegation at the 2007 meeting of the Cyber crime Committee.

- *Supplementing the Convention's Standards:* A new model law could go beyond the standards defined by the Convention on Cyber crime and, for example, criminalise certain Cyber crime-related acts and define procedural instruments that are not yet covered by the Convention. Since, 2001, a number of important developments have taken place. When the Convention was drafted, "phishing", "identity theft" and offences related to online games and social networks were not as relevant as they have since become. A new model law could continue the harmonisation process by including further offences with transnational dimension.

In this regard, the ITU Toolkit for Cyber crime Legislation aims to provide countries with reference material that can assist in the establishment of a legislative framework to deter cyber crime. It highlights the importance for countries to harmonise their legal frameworks in order to more effectively combat cyber crime and facilitate international cooperation. Development of the ITU Toolkit for Cyber crime Legislation is by a multidisciplinary international group of experts and a first draft was made available in early 2009.

THE RELATIONSHIP BETWEEN INTERNATIONAL AND NATIONAL LEGISLATIVE APPROACHES

Cyber crime is a truly transnational crime. With regard to the fact that offenders can, in general, target users in any country in the world, international cooperation of law enforcement agencies is an essential requirement for international cyber crime investigations. The investigations require the means of cooperation and depend on the harmonisation of laws. Due to the common principle of dual criminality, an effective cooperation firstly requires a harmonisation of substantive criminal law provisions to prevent

safe havens. In addition, it is necessary to harmonise investigation instruments to ensure that all countries involved in an international investigation have the necessary investigative instruments in place to carry out the investigations. Finally, an effective cooperation of law enforcement agencies requires effective procedures related to practical aspects. The importance of harmonisation triggers and the need to incorporate participation in the global harmonisation process is therefore at least a tendency, if not a necessity, for any national Anti-Cyber crime Strategy.

Reasons for the Popularity of National Approaches

Despite the widely recognised importance of harmonisation, the process of implementing international legal standards is far away from being completed. One of the reasons why national approaches play an important role in the fight against cyber crime is that the impact of the crimes is not universally the same. One example is the approach taken to fight spam. Spam-related e-mails especially affect developing countries and this issue was analysed in an OECD report. Due to scarcer and more expensive resources, spam turns out to be a much more serious issue in developing countries than in western countries. The different impacts of cyber crime, together with existing legal structures and traditions, are the main reasons for a significant number of legislative initiatives at the national level which are not, or only partly, dedicated to the implementation of international standards.

International vs. National Solutions

In times of technical globalisation this may seem like a slightly surprising discussion as anybody wishing to connect to the Internet needs to make use of the (technical) standard protocols in place. Single standards are an essential requirement for the operation of the networks. However, unlike technical standards, the legal standards still differ. It must be questioned whether national approaches can still work, given the international dimension of cyber crime. The question is relevant for all national and regional approaches that

implement legislation that are not in line with existing international standards. A lack of harmonisation can seriously hinder international investigations, whereas national and regional approaches going beyond the international standards avoid problems and difficulties in conducting international investigations. There are two main reasons for a growing number of regional and national approaches.

The first is legislative speed. The Council of Europe can neither force any of its Member States to sign the Convention on Cyber crime nor can it force a signatory of the Convention to ratify it. The harmonisation process is therefore often considered to be slow compared to national and regional legislative approaches.

Unlike the Council of Europe, the European Union has means to force Member States to implement framework decisions and directives. This is the reason why a number of European Union countries that signed the Convention on Cyber crime in 2001, but have not yet ratified it, have nevertheless implemented the 2005 EU Framework Decision on Attacks against Information Systems. The second reason is related to national and regional differences. Some offences are only criminalised in certain countries in a region. Examples are religious offences. Although it is unlikely that an international harmonisation of criminal law provisions related to offences against religious symbols would be possible, a national approach can in this regard ensure that legal standards in one country can be maintained.

Difficulties of National Approaches

National approaches face a number of problems. With regard to traditional crimes the decision by one, or a few countries, to criminalise certain behaviours can influence the ability of offenders to act in those countries.

However, when it comes to Internet-related offences the ability of a single country to influence the offender is much smaller as the offender can, in general, act from any place with a connection to the network. If they act from a country that does not criminalise the certain behaviour, international

investigations as well as extradition requests will very often fail. One of the key aims of international legal approaches is therefore to prevent the creation of those safe havens by providing and applying global standards.

As a result national approaches in general require additional side measures to be able to work. The most popular side measures:

- **Criminalisation of the User in Addition to the Supplier of Illegal Content:** A second approach is the regulation and even criminalisation of offering certain services within the jurisdiction that are used for criminal purposes. This solution goes beyond the first approach as it concerns businesses and organisations that offer neutral services that are used for legal as well as illegal activities. An example of such an approach is the United States Unlawful Internet Gambling Enforcement Act of 2006. Closely related to this measure, is the establishment of obligations to filter certain content available on the Internet. Such an approach was discussed within the famous Yahoo-decision and is currently discussed in Israel, where Access providers should be obliged to restrict the access to certain adult-content Web site. Attempts to control Internet content are not limited to adult-content; some countries use filter technology to restrict access to websites that address political topics. OpenNet Initiative reports that censorship is practised by about two dozen countries.

Chapter 10

Legal Response

SUBSTANTIVE CRIMINAL LAW

Illegal Access (Hacking)

Since the development of computer networks, their ability to connect computers and offer users access to other computer systems, computers have been used by hackers for criminal purposes. There is substantial variation in hackers' motivations. Hackers need not be present at the crime scene; they just need to circumvent the protection securing the network.

In many cases of illegal access, the security systems protecting the physical location of network hardware are more sophisticated than the security systems protecting sensitive information on networks, even in the same building. The illegal access to computer systems hinders computer operators from managing, operating and controlling their systems in an undisturbed and uninhibited manner. The aim of protection is to maintain the integrity of computer systems.

It is vital to distinguish between illegal access and subsequent offences (such as data espionage), as legal provisions have a different focus of protection. In most cases, illegal access (where law seeks to protect the integrity of the computer system itself) is not the end-goal, but rather a first step towards further crimes, such as modifying or obtaining stored data (where law seeks to protect the integrity and confidentiality of the data). The question is whether the act of illegal access should be criminalised, in addition to subsequent offences? Analysis of the various approaches to the

criminalisation of illegal computer access at the national level shows that enacted provisions sometimes confuse illegal access with subsequent offences, or seek to limit the criminalisation of the illegal access to grave violations only.

Some countries criminalise mere access, while others limit criminalisation to offences only in cases where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data was obtained, modified or damaged. Other countries do not criminalise the access itself, but only subsequent offences. Opponents to the criminalisation of illegal access refer to situations where no dangers were created by mere intrusion, or where acts of “hacking” have led to the detection of loopholes and weaknesses in the security of targeted computer systems.

Convention on Cyber crime

The Convention on Cyber crime includes a provision on illegal access protecting the integrity of the computer systems by criminalising the unauthorised access to a system. Noting inconsistent approaches at the national level, the Convention offers the possibility of limitations that – at least in most cases – enable countries without legislation to retain more liberal laws on illegal access.

The Provision

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

The Covered Acts

The term “access” does not specify a certain means of communication, but is open-ended and open to further

technical developments. It shall include all means of entering another computer system, including Internet attacks, as well as illegal access to wireless networks. Even unauthorised access to computers that are not connected to any network (*e.g.*, by circumventing a password protection) are covered by the provision.

This broad approach means that illegal access not only covers future technical developments, but is also covers secret data accessed by insiders and employees. The second sentence of Article 2 offers the possibility of limiting the criminalisation of illegal access to access over a network. The illegal acts and protected systems are thus defined in a way that remains open to future developments. The Explanatory Report lists hardware, components, stored data, directories, traffic and content-related data as examples of the parts of computer systems that can be accessed.

Mental Element

Like all other offences defined by the Convention on Cyber crime Art. 2 requires that the offender is carrying out the offences intentionally. The Convention does not contain a definition of the term “internationally”. In the Explanatory Report the drafters pointed out that the definition of “intentionally” should happen on a national level.

Without Right

Access to a Computer can only be prosecuted under Article 2 of the Convention, if it should happen “without right”. Access to a system permitting free and open access by the public or access to a system with the authorisation of the owner or other rights-holder is not “without right”.

In addition to the subject of free access, the legitimacy of security testing procedures is also addressed. Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in the security measures were wary of the possibility of criminalisation under illegal access. Despite the fact that these professionals generally work with the permission of the owner and therefore

act legally, the drafters of the Convention emphasised that “testing or protection of the security of a computer system authorised by the owner or operator, are with right”. The fact, that the victim of the crime handed out a password or similar access code to the offender does not necessary mean that the offender then acted with right when he accessed the computer system of the victim.

If the offender persuaded the victim to disclose a password or access code due to a successful social engineering approach it is necessary to verify if the authorisation given by the victim does cover the act carried out by the offender. In general this is not the case and the offender therefore acts without right.

Restrictions and Reservations

As an alternative to the broad approach, the Convention offers the possibility of restricting criminalisation with additional elements, listed in the second sentence. The procedure of how to utilise this reservation is laid down in Article 42 of the Convention. Possible reservations relate to security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or requirements that the offence be committed against a computer system through a network. A similar approach can be found in the EU Framework Decision on Attacks against Information Systems.

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in Sec. 5 of the 2002 Commonwealth Model Law:

- Sec. 5.: A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding, or a fine not exceeding or both.

The main difference to the Convention on Cyber crime is the fact that Sec. 5 of the Commonwealth Model Law does, unlike Art. 2 Convention on Cyber crime, not contain options to make reservations.

The informal 1999 Stanford Draft Convention recognises illegal access as one of those offences the signatory states should criminalise.

The Provision

- Art. 3 – Offences:
 - 1. Offences under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognised authority, permission, or consent:
 - (c) enters into a cyber system for which access is restricted in a conspicuous and unambiguous manner;

The Covered Acts

The draft provision shows a number of similarities to Art. 2 of the Convention on Cyber crime. Both require an intentional act that is committed without right/without authority. In this context requirement of the draft provision (*“without legally recognised authority, permission, or consent”*) is more precise than the term *“without right”* used Convention on Cyber crime and explicitly aims to incorporate the concept of selfdefence. The main difference to the Convention is the fact that the draft provision uses the term *“cyber system”*.

The cyber system is defined in Art. 1, paragraph 3 of the Draft Convention. It covers any computer or network of computers used to relay, transmit, coordinate, or control communications of data or Programmes.

This definition shows many similarities to the definition of the term *“computer system”* provided by Art. 1 a) Convention on Cyber crime. Although the Draft Convention refers to acts related to the exchange of data and does therefore primarily focus on network based computer systems both definitions include interconnected computer as well as stand alone machines.

The Convention on Cyber crime as well as the Commonwealth Model Law and the Stanford Draft Convention provide legal solutions for illegal interception only. It is questionable whether Article 3 of the Convention on Cyber crime applies to other cases than those where offences are carried out by intercepting data transfer processes. The question of whether illegal access to information stored on a hard disk is covered by the Convention was discussed with great interest.

Since a transfer process is needed, it is likely that Art. 3 of the Convention on Cyber crime does not cover forms of data espionage other than the interception of transfer processes. One issue frequently discussed in this context is the question if the criminalisation of illegal accesses renders the criminalisation of data espionage unnecessary. In those cases where the offender has legitimate access to a computer system (e.g. because he is ordered to repair it) and on this occasion (in violation of the limited legitimating) copies files from the system, the act is in general not covered by the provisions criminalising illegal access.

Given that much vital data is today stored in computer systems, it is essential to evaluate whether existing mechanisms to protect data are adequate or whether other criminal law provision are necessary to protect the user from data espionage. Today, computer users can use various hardware devices and software tools in order to protect secret information.

They can install firewalls, access control systems or encrypt stored information and by this decrease the risk of data espionage. Although user-friendly devices are available, requiring only limited knowledge by users, truly effective protection of data on a computer system often requires knowledge that few users have. Especially data stored on private computer systems is often not adequately protected against data espionage. Therefore criminal law provisions can offer an additional protection.

Some countries have decided to extend the protection that is available through technical measures by criminalising data espionage. There are two main approaches. Some countries follow a narrow approach and criminalise data espionage, only where specific secret information is obtained - an example is 18 U.S.C § 1831, that criminalises economic espionage. The provision does not only cover data espionage, but other ways of obtaining secret information as well.

Economic Espionage

- (a) In General — Whoever, intending or knowing that the Offence will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—
 - (1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
 - (2) Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
 - (3) Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
 - (4) Attempts to commit any Offence described in any of paragraphs (1) through (3); or
 - (5) Conspires with one or more other persons to commit any Offence described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.

- (b) Organizations — Any organization that commits any Offence described in subsection (a) shall be fined not more than \$10,000,000.

Other countries have adopted a broader approach and criminalised the act of obtaining stored computer data, even if they do not contain economic secrets.

Section 202a. Data Espionage

- (1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorised access, shall be liable to imprisonment for a term not exceeding three years or to a fine.
- (2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

This provision not only covers economic secrets, but stored computer data in general. In terms of its objects of protection, this approach is broader compared to § 1831 USC, but the application of the provision is limited as obtaining data is only criminalised where data are specially protected against unauthorised access. The protection of stored computer data under German criminal law is thus limited to persons or businesses that have taken measures to avoid falling victim to such offences.

Relevance of Such Provision

The implementation of such provision is especially relevant with regard to cases, where the offender was authorised to access a computer system (e.g. because he was ordered to fix a computer problem) and then abused the authorisation to illegally obtain information stored on the computer system. With regard to the fact that the permission covers the access to the computer system it is in general not possible to cover with provisions criminalising the illegal access.

Without Right

The application of data espionage provisions in general requires that the data was obtained without the consent of the

victim. The success of phishing attacks clearly demonstrates the success of scams based on the manipulation of users. Due to the consent of the victim offenders who succeed in manipulating of users to disclose secret information cannot be prosecuted on the basis of the above mentioned provisions.

Illegal Interception

The use of ICTs is accompanied by several risks related to the security of information transfer. Unlike classic mail order operations within a country, data transfer processes over the Internet involve numerous providers and different points where the data transfer process could be intercepted. The weakest point for intercept remains the user, especially users of private home computers, who are often inadequately protected against external attacks.

As offenders generally always aim for the weakest point, the risk of attacks against private users is great, all the more so given:

- The development of vulnerable technologies;
- The rising relevance of personal information for offenders.

New network technologies (such as “wireless LAN”) offer several advantages for Internet access. Setting up a wireless network in a private home, for example, allows families to connect to the Internet from anywhere inside a given radius, without the need for cable connections. But the popularity of this technology and resulting comfort is accompanied by serious risks to network security.

If an unprotected wireless network is available perpetrators can log on to this network and use it for criminal purposes without the need to get access to a building. They simply need to get inside the radius of the wireless network to launch an attack. Field tests suggest that in some areas as many as 50 per cent of private wireless networks are not protected against unauthorised interception or access. In most cases, lack of protection arises from a lack of knowledge as to how to configure protection measures. In the past, perpetrators concentrated mainly on business networks for illegal

interceptions. Interception of corporate communications was more likely to yield useful information, than data transferred within private networks. The rising number of identity thefts of private personal data suggests that the focus of the perpetrators may have changed. Private data such as credit card numbers, social security numbers, passwords and bank account information are now of great interest to offenders.

The Convention on Cyber crime

The Convention on Cyber crime includes a provision protecting the integrity of non-public transmissions by criminalising their unauthorised interception. This provision aims to equate the protection of electronic transfers with the protection of voice conversations against illegal tapping and/or recording that currently already exists in most legal systems.

The Provision

- Article 3 – Illegal interception: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The Covered Acts

The applicability of Article 3 is limited to the interception of transmissions realised by technical measures. Interceptions related to electronic data can be defined as any act of acquiring data during a transfer process. The question if illegal access to information stored on a hard disk is covered by the provision is controversially discussed. In general the provision only applies to the interception of transmissions - access to stored

information is not considered as an interception of a transmission.

The fact that the application of the provision is discussed even in cases where the offender physically access a standalone computer system partly arises as a result of the fact, that the Convention on Cyber crime does not contain a provision related to data espionage and the Explanatory Report to the Convention contains two slightly imprecise explanations with regard to the application of Art. 3:

- The Explanatory Report first of all points out that the provision covers communication processes taking place within a computer system. However, this still leaves open the question of whether the provision should only apply in cases where victims send data that are then intercepted by offenders or whether it should apply also when the offender himself operates the computer.
- The guide points out that interception can be committed either indirectly through the use of tapping devices or "through access and use of the computer system". If offenders gain access to a computer system and use it to make unauthorised copies of stored data on an external disc drive, where the act leads to a data transfer (sending data from the internal to the external hard disc), this process is not *intercepted*, but rather *initiated*, by offenders. The missing element of technical interception is a strong argument against the application of the provision in cases of illegal access to stored information.

The term "transmission" covers all data transfers, whether by telephone, fax, e-mail or file transfer. The offence established under Article 3 applies only to non-public transmissions. A transmission is "non-public", if the transmission process is confidential. The vital element to differentiate between public and non-public transmissions is not the nature of the data transmitted, but the nature of the transmission process itself. Even the transfer of publicly available information can be considered criminal, if the parties involved in the transfer

intend to keep the content of their communications secret. Use of public networks does not exclude “nonpublic” communications.

Mental Element

Like all other offences defined by the Convention on Cyber crime, Article 3 requires that the offender is carrying out the offences intentionally. The Convention does not contain a definition of the term “internationally”. In the Explanatory Report the drafters pointed out that the definition of “intentionally” should happen on a national level.

Without Right

The interception of communication can only be prosecuted under Article 3 of the Convention, if it should happen “without right”.

The drafters of the Convention provided a set of examples for interceptions that are not carried out without right:

- Action on the basis instructions or by authorisation of the participants of the transmission;
- Authorised testing or protection activities agreed to by the participants;
- Lawful interception on the basis of criminal law provisions or in the interests of national security.

Another issue raised within the negotiation of the Convention was the question if the use of cookies would lead to criminal sanctions based on Art. 3. The drafters pointed out that common commercial practices (such as cookies) are not considered to be interceptions without right.

Restrictions and Reservations

Article 3 offers the option of restricting criminalisation by requiring additional elements listed in the second sentence, including a “dishonest intent” or relation to a computer system connected to another computer system.

Commonwealth Computer and Computer Related Crimes Model Law

A similar approach can be found in Sec. 8 of the 2002

Commonwealth Model Law.

- Sec. 8.: A person who, intentionally without lawful excuse or justification, intercepts by technical means:
 - (a) Any non-public transmission to, from or within a computer system;
 - (b) Electromagnetic emissions from a computer system that are carrying computer data; commits an offence punishable, on conviction, by imprisonment for a period not exceeding, or a fine not exceeding, or both.

Stanford Draft Convention

The informal 1999 Stanford Draft Convention does not explicitly criminalise the interception of computer data.

Data Interference

The protection of tangible, or physical, objects against intentional damage is a classic element of national penal legislation. With continuing digitalisation, more critical business information is stored as data. Attacks or obtaining of this information can result in financial losses. Besides deletion, the alteration of such information could also have major consequences. Previous legislation has in some not completely brought the protection of data in line with the protection of tangible objects. This enabled offenders to design scams that do not lead to criminal sanctions.

Convention on Cyber crime

In Article 4, the Convention on Cyber crime includes a provision that protects the integrity of data against unauthorised interference. The aim of the provision is to fill existing gaps in some national penal laws and to provide computer data and computer programmes with protections similar to those enjoyed by tangible objects against the intentional infliction of damage.

The Provision

- Article 4 – Data interference:

- (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
 - (2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
- The covered acts:
 - The terms “damaging” and “deterioration” mean any act related to the negative alteration of the integrity of information content of data and programmes;
 - “Deleting” covers acts where information is removed from storage media and is considered comparable to the destruction of a tangible object. While providing the definition the the drafters of the Convention did not differentiate between the various ways data can be deleted. Dropping a file to the virtual trash bin does not remove the file from the hard disk. Even “emptying” the trash bin does not necessary remove the file. It is therefore uncertain if the ability to recover a deleted file hinders the application of the provision.
 - “Suppression” of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way. The application of the provision is especially discussed with regard to Denial-of-Service attacks. During the attack the data provided on the targeted computer system are not available anymore for potential user as well as the owner of the computer system.

- The term “alteration” covers the modification of existing data, without necessarily lowering the serviceability of the data. This act is especially covering the installation of malicious software like spyware, viruses or adware on the victim’s computer.

Mental Element

Like all other offences defined by the Convention on Cyber crime Article 4 requires that the offender is carrying out the offences intentionally. The Convention does not contain a definition of the term “internationally”. In the Explanatory Report the drafters pointed out that the definition of “intentionally” should happen on a national level.

Without Right

The acts must be committed “without right”. The right to alter data was discussed, especially in the context of “remailers”. Remailers are used to modify certain data for the purpose of facilitating anonymous communications. The Explanatory Reports mention that, in principle, these acts are considered a legitimate protection of privacy and can thus be considered as being undertaken with authorisation.

Restrictions and Reservations

Article 4 offers the option of restricting criminalisation by limiting it to cases where serious harm arises, a similar approach to the EU Framework Decision on Attacks against Information Systems, which enables Member States to limit the applicability of the substantive criminal law provision to “cases which are not minor”.

Commonwealth Computer and Computer Related Crimes Model Law

An approach in line with Art. 4 Convention on Cyber crime can be found in Sec. 8 of the 2002 Commonwealth Model Law.

Sec. 6

- (1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:
 - (a) Destroys or alters data; or
 - (b) Renders data meaningless, useless or ineffective; or
 - (c) Obstructs, interrupts or interferes with the lawful use of data; or
 - (d) Obstructs, interrupts or interferes with any person in the lawful use of data; or
 - (e) Denies access to data to any person entitled to it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding or a fine not exceeding [amount], or both.
- (2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

Stanford Draft Convention

The informal 1999 Stanford Draft Convention contains two provisions that criminalise acts related to interference with computer data.

The Provision

Art. 3:

1. Offences under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognised authority, permission, or consent:
 - (a) Creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or Programmes in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform

- functions or activities not intended by its owner and considered illegal under this Convention;
- (b) Creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data in a cyber system for the purpose and with the effect of providing false information in order to cause substantial damage to persons or property;

The Covered Acts

The main difference between the Convention on Cyber crime and the Commonwealth Model Law and the approach of the Draft Convention is the fact, that Draft Convention does only criminalise the interference with data if this interferes with the functioning of a computer system (Art. 3, paragraph 1a) or if the act is committed with the purpose of providing false information in order to causing damage to a person or property (Art. 3, paragraph 1b). Therefore the draft law does not criminalise the deletion of a regular text document of a data storage device as this does neither influence the functioning of a computer nor does it provide false information. The Convention on Cyber crime and the Commonwealth Model Law both follow a broader approach by protecting the integrity of computer data without the mandatory requirement of further effects.

System Interference

People or businesses offering services based on ICTs depend on the functioning of their computer systems. The lack of availability of webpages that are victim to Denial-of-Service (DOS) attacks demonstrates how serious the threat of attack is. Attacks like these can cause serious financial losses and affect even powerful systems. Businesses are not the only targets. Experts around the world are currently discussing possible scenarios of “cyber terrorism” that take into account attacks against critical infrastructures such as power supplies and telecommunication services.

Convention on Cyber Crime

To protect access of operators and users to ICTs, the Convention on Cyber crime includes a provision in Article 5 criminalising the intentional hindering of lawful use of computer systems.

The Provision

Article 5 – System interference:

- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The Covered Acts

The application of the provision requires that the functioning of a computer system was hindered.

- “Hindering” means any act interfering with the proper functioning of the computer system. The application of the provision is limited to cases where hindering is carried out by one of the mentioned acts.

The list of acts by which the functioning of the computer system was influenced in a negative way is conclusive.

- The term “inputting” is neither defined by the Convention itself, nor by the drafters of the Convention. With regard to the fact, the transmitting is mentioned as an additional act in Art. 5 the term “inputting” could be defined as any act related to use of physical input-interfaces to transfer information to a computer system whereas the term “transmitting” is covering acts that go along with the remote input of data.
- The terms “damaging” and “deteriorating” are overlapping and defined by the drafters of the Convention in the Explanatory Report with regard to Art. 4 as negative alteration of the integrity of information content of data and programmes.

- The term “deleting” was also defined by the drafters of the Convention and the Explanatory Report with regard to Article 4 covers acts where information is removed from storage media.
- The term “alteration” covers the modification of existing data, without necessarily lowering the serviceability of the data.
- “Suppression” of computer data denotes an action that affects the availability of data to the person with access to the medium, where the information is stored in a negative way.

In addition, the provision applies limited to cases where hindering is “serious”. It is the parties’ responsibility to determine the criteria to be fulfilled in order for the hindering to be considered as serious. Possible restrictions under national law could include a minimum amount of damage, as well as limitation of criminalisation to attacks against important computer systems.

Application of the Provision with Regard to Spam

It was discussed whether the problem of spam e-mail could be addressed under Article 5, since spam can overload computer systems. The drafters stated clearly that spam may not necessarily lead to “serious” hindering and that “conduct should only be criminalised where the communication is intentionally and seriously hindered”. The drafters also noted that parties may have a different approach to hindrance under their own national legislation *e.g.*, by making acts of interference administrative offences or subject to sanction.

Mental Element

Like all other offences defined by the Convention on Cyber crime Art. 5 requires that the offender is carrying out the offences intentionally. This includes the intent to carry out one of listed acts as well as the intention to seriously hinder the functioning of a computer system. The Convention does not contain a definition of the term “internationally”. In the Explanatory Report the drafters pointed out that the definition

of “intentionally” should happen on a national level.

Without Right

The act needs to be carried out “without right”. Network administrators and security companies testing the protection of computer systems were afraid of the possible criminalisation of their work. These professionals work with the permission of the owner and therefore act legally. In addition, the drafters of the Convention explicitly mentioned that testing the security of a computer system based on the authorisation of the owner is not without right.

Restrictions and Reservations

Unlike Articles 2 – 4, Article 5 does not contain an explicit possibility of restricting the application of the provision to implementation in the national law.

Nevertheless, the responsibility of the parties to define the gravity of the offence gives them the possibility to restrict its application. A similar approach can be found in the European Union Framework Decision on Attacks against Information Systems.

Commonwealth Computer and Computer Related Crimes Model Law

An approach in line with Article 5 of the Convention on Cyber crime can be found in Sec. 7 of the 2002 Commonwealth Model Law.

Sec 7:

- (1) A person who intentionally or recklessly, without lawful excuse or justification:
 - (a) Hinders or interferes with the functioning of a computer system;
 - (b) Hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not

exceeding [amount], or both.

In subsection (1) "hinder", in relation to a computer system, includes but is not limited to:

- (a) Cutting the electricity supply to a computer system;
- (b) Causing electromagnetic interference to a computer system;
- (c) Corrupting a computer system by any means;
- (d) Inputting, deleting or altering computer data.

The main differences to the Convention is the fact, that based on Sec. 7 of the Commonwealth Model Law even reckless acts are criminalised. With this approach the Model Law even goes beyond the requirements of the Convention on Cyber crime. Another difference is the fact, that the definition of "hindering" in Sec. 7 of the Commonwealth Model Law lists more acts compared to Article 5 of the Convention on Cyber crime.

Stanford Draft Convention

The informal 1999 Stanford Draft Convention contains a provision that criminalises acts related to the interference with computer systems.

The Provision

Art. 3:

1. Offenses under this Convention are committed if any person unlawfully and intentionally engages in any of the following conduct without legally recognised authority, permission, or consent:
 - (a) Creates, stores, alters, deletes, transmits, diverts, misroutes, manipulates, or interferes with data or Programmes in a cyber system with the purpose of causing, or knowing that such activities would cause, said cyber system or another cyber system to cease functioning as intended, or to perform functions or activities not intended by its owner and considered illegal under this Convention.

The Covered Acts

The main difference between the Convention on Cyber crime and the Commonwealth Model Law and the approach of the Draft Convention is the fact, that Draft Convention does cover any manipulation of computer systems while the Convention on Cyber crime and the Commonwealth Model Law limit the criminalisation to the hindering of the functioning of a computer system.

Erotic or Pornographic Material

The criminalisation and gravity of criminalisation of illegal content and sexually-explicit content varies between countries. The parties that negotiated the Convention on Cyber crime focused on the harmonisation of laws regarding child pornography and excluded the broader criminalisation of erotic and pornographic material. Some countries have addressed this problem by implementing provisions that criminalise the exchange of pornographic material through computer systems. However, the lack of standard definitions makes it difficult for law enforcement agencies to investigate those crimes, if offenders act from countries that have not criminalised the exchange of sexual content.

Examples

One example of the criminalisation of the exchange of pornographic material is Section 184 of the German Penal Code:

- Section 184 Dissemination of Pornographic Writings:
 - (1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):
 1. Offers, gives or makes them accessible to a person under eighteen years of age;
 2. Displays, posts, presents or otherwise makes them accessible at a place accessible to persons under eighteen years of age, or into which they can see;
 3. Offers or gives them to another in retail trade outside of the business premises, in kiosks or

other sales areas which the customer usually does not enter, through a mail-order business or in commercial lending libraries or reading circles;

3a. offers or gives them to another by means of commercial rental or comparable commercial furnishing for use, except for shops which are not accessible to persons under eighteen years of age and into which they cannot see;

4. Undertakes to import them by means of a mail-order business;
5. Publicly offers, announces, or commends them at a place accessible to persons under eighteen years of age or into which they can see, or through dissemination of writings outside of business transactions through normal trade outlets;
6. Allows another to obtain them without having been requested to do by him;
7. Shows them at a public film showing for compensation requested completely or predominantly for this showing;
8. Produces, obtains, supplies, stocks, or undertakes to import them in order to use them or copies made from them within the meaning of numbers 1 through 7 or to make such use possible by another;
9. Undertakes to export them in order to disseminate them or copies made from them abroad in violation of the applicable penal provisions there or to make them publicly accessible or to make such use possible, shall be punished with imprisonment for not more than one year or a fine.

This provision is based on the concept that trade and other exchange of pornographic writings should not be criminalised,

if minors are not involved. On this basis, the law aims to protect the undisturbed development of minors. If access to pornography has a negative impact on the development of minors is controversially discussed. The exchange of pornographic writings among adults is not criminalised by Section 184. The term "writing" covers not only traditional writings, but also digital storage. Equally, making "them accessible" not only applies to acts beyond the Internet, but covers cases where offenders make pornographic content available on websites.

One example of an approach that goes beyond this and criminalises any sexual content is Section 4.C.1, Philippines draft House Law Bill No. 3777 of 2007.

- *Sec. 4.C1: Offenses Related to Cybersex* – Without prejudice to the prosecution under Republic Act No. 9208 and Republic Act No. 7610, any person who in any manner advertises, promotes, or facilitates the commission of cybersex through the use of information and communications technology such as but not limited to computers, computer networks, television, satellite, mobile telephone, [...]
- *Section 3i: Cybersex or Virtual Sex* – refers to any form of sexual activity or arousal with the aid of computers or communications network

This provision follows a very broad approach, as it criminalises any kind of sexual advertisement or facilitation of sexual activity carried out over the Internet. Due to the principle of dual criminality international investigations with regard to such broad approaches go along with difficulties.

Child Pornography

The Internet is becoming the main instrument for the trade and exchange of material containing child pornography. The major reasons for this development are the speed and efficiency of the Internet for file transfers, its low production and distribution costs and perceived anonymity. Pictures placed on a webpage can be accessed and downloaded by millions of users worldwide. One of the most important reasons for the

“success” of web pages offering pornography or even child pornography is the fact that Internet users are feeling less observed while sitting in their home and downloading material from the Internet. Unless the users made use of means of anonymous communication the impression of a missing traceability is wrong. Most Internet users are simply unaware of the electronic trail they leave while surfing.

Council of Europe Convention on Cyber Crime

In order to improve and harmonise the protection of children against sexual exploitation, the Convention includes an Article addressing child pornography.

The Provision

- Article 9 – Offences related to child pornography:
 - (1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a) Producing child pornography for the purpose of its distribution through a computer system;
 - b) Offering or making available child pornography through a computer system;
 - c) Distributing or transmitting child pornography through a computer system;
 - d) Procuring child pornography through a computer system for oneself or for another person;
 - e) Possessing child pornography in a computer system or on a computer-data storage medium.
 - (2) For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
 - a) a minor engaged in sexually explicit conduct;
 - b) a person appearing to be a minor engaged in sexually explicit conduct;

- c) Realistic images representing a minor engaged in sexually explicit conduct.
- (3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
- (4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d. and e, and 2, sub-paragraphs b. and c.

Most countries already criminalise the abuse of children, as well as the traditional methods of distribution of child pornography. The Convention is thus not limited to the closing of gaps in national criminal law - it also seeks to harmonise differing regulation.

Three controversial elements are covered by Article 9:

- The age of the person involved;
- The criminalisation of the possession of child pornography;
- The creation or integration of fictional images.

Age Limit for Minors

One of the most important differences between national legislation is the age of the person involved. Some states define the term 'minor' in relation to child pornography in their national law in accordance with the definition of a 'child' in Article 1 of the UN Convention on the Rights of the Child as all persons less than 18 years old. Other countries define minors as a person under 14 years old. A similar approach is found in the 2003 EU Council Framework Decision on combating the sexual exploitation of children and child pornography and the 2007 Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse. Emphasizing the importance of a uniform international standard regarding age, the Convention defines the term according to the UN Convention. However, in recognition of the huge differences in the existing national laws, the Convention permits parties to require a different age limit of not lower than 16 years.

Criminalisation of the Possession of Child Pornography

Criminalisation of possession of child pornography also differs between national legal systems. The demand for such material could result in their production on an ongoing basis. The possession of such material could encourage the sexual abuse of children, so drafters suggest that one effective way to curtail the production of child pornography is to make possession illegal.

However, the Conventions enable the parties in Paragraph 4 to exclude the criminalisation of mere possession, by restricting criminal liability to the production, offer and distribution of child pornography only.

The Creation or Integration of Fictional Images

Although the drafters sought to improve the protection of children against sexual exploitation, the legal interests covered by Paragraph 2 are broader. Paragraph 2(a) focuses directly on protection against child abuse. Paragraphs 2(b) and 2(c) cover images that were produced without violating children's rights – *e.g.*, images that have been created through the use of 3D modelling software. The reason for the criminalisation of fictive child pornography is that fact that these images can - without necessarily creating harm to a real 'child' - be used to seduce children into participating in such acts.

Mental Element

Like all other offences defined by the Convention on Cyber crime Article 9 requires that the offender is carrying out the offences intentionally. In the Explanatory Report the drafters explicitly pointed out that the interaction with child pornography without any intention is not covered by the Convention. A missing intention can especially be relevant if the offender accidentally opened a webpage with child pornography images and despite the fact that he immediately closed the Web site some images were stored in temp-folders or cache-files.

Without Right

The acts related to child pornography can only be prosecuted under Article 9 of the Convention, if it should happen “without right”. The drafters of the Convention did not further specify in which cases the user is acting with authorisation. In general the act is not carried out “without right” only if members of law enforcement agencies are acting within an investigation.

Council of Europe Convention on the Protection of Children

Another approach to criminalise acts related to Child Pornography is Art. 20 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

The Provision

Article 20 – Offences concerning child pornography:

- (1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:
 - a) Producing child pornography;
 - b) Offering or making available child pornography;
 - c) Distributing or transmitting child pornography;
 - d) Procuring child pornography for oneself or for another person;
 - e) Possessing child pornography;
 - f) Knowingly obtaining access, through information and communication technologies, to child pornography.
- (2) For the purpose of the present article, the term “child pornography” shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes.

- (3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:
 - Consisting exclusively of simulated representations or realistic images of a non-existent child;
 - Involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.
- (4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f

The Covered Acts

The provision is based on Art. 9 Convention on Cyber crime and therefore up to a large degree comparable to this provision. The main difference is the fact, that the Convention on Cyber crime is focusing on the criminalisation of acts related to information and communication services (“producing child pornography for the purpose of its distribution through a computer system”) while the Convention on the Protection of Children is mainly following a broader approach (“producing child pornography”) and even covers acts that are not related to computer networks.

Despite the similarities with regard to the covered acts, Art. 20 of the Convention on the Protection of Children contains one act that is not covered by the Convention. Based on Art. 20, paragraph 1f of the Convention on the Protection of Children the act of obtaining access to child pornography through a computer is criminalised.

This enables law enforcement agencies to prosecute offenders in cases where they are able to prove that the offender opened websites with child pornography but they are unable to prove that the offender downloaded material. Such difficulties in collecting evidence do for example arise if the offender is using encryption technology to protect downloaded files on his storage media. The Explanatory Report

to the Convention on the Protection of children points out that the provision should also be applicable in cases, where the offender does only watch child pornography pictures online without downloading them. In general opening a Web site does automatically initiate a download process—often without the knowledge of the user. The case mentioned in the Explanatory Report is therefore only relevant in those cases where a download in the background is not taking place.

Commonwealth Model Law

An approach in line with Art. 9 Convention on Cyber crime can be found in Sec. 10 of the 2002 Commonwealth Model Law.

Sec. 10:

- (1) A person who, intentionally, does any of the following acts:
 - (a) Publishes child pornography through a computer system;
 - (b) Produces child pornography for the purpose of its publication through a computer system; or
 - (c) Possesses child pornography in a computer system or on a computer data storage medium; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.
- (2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose.
- (3) In this section: “child pornography” includes material that visually depicts:
 - (a) A minor engaged in sexually explicit conduct; or
 - (b) A person who appears to be a minor engaged in sexually explicit conduct; or
 - (c) Realistic images representing a minor engaged in

sexually explicit conduct. "minor" means a person under the age of [x] years. "publish" includes:

- (a) Distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;
- (b) Have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or
- (c) Print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).

The main differences to the Convention on Cyber crime is the fact, that the Commonwealth Model Law does not provide a fixed definition of the term minor and leaves it to the Member States to define the age limit.

Stanford Draft Convention

The informal 1999 Stanford Draft Convention does not contain a provision criminalising the exchange of child pornography through computer systems. The drafters of the Convention pointed out, that in general no type of speech, or publication, is required to be treated as criminal under the Stanford Draft. Recognising different national approaches the drafters of the Convention left it to the states to decide about this aspect of criminalisation.

Hate Speech, Racism

Not all countries criminalise hate speech.

Convention on Cyber Crime

Since the parties negotiating the Convention on Cyber crime could not agree on a common position on the criminalisation of such material, provisions related to this topic were integrated into a separate First Protocol to the Convention on Cyber crime.

The Provision

Article 3 – Dissemination of racist and xenophobic material through computer systems:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.
3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat:

- Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - Threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law,
 - (i) Persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or
 - (ii) A group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult:

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - Insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.
2. A Party may either:
 - a. Require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or
 - b. Reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity:

1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:
 - Distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.
2. A Party may either:
 - a. Require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed

- with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
- b. Reserve the right not to apply, in whole or in part, paragraph 1 of this article.

One of the main difficulties related to provisions criminalising xenophobic material is to keep a balance between ensuring freedom of speech on the one hand and preventing the violation of the rights of individuals or groups on the other hand. Without going into detail the difficulties within the negotiation of the Convention on Cyber crime and the status of the signatures/ ratifications of the Additional Protocol demonstrates, that the different extend of the protection of freedom of speech is hindering a harmonisation process. Especially with regard to the common principle of dual criminality a missing harmonisation leads to difficulties in the enforcement in cases with an international dimension.

Stanford Draft Convention

The informal 1999 Stanford Draft Convention does not include a provision criminalising hate speech. The drafters of the Convention pointed out, that in general no type of speech, or publication, is required to be treated as criminal under the Stanford Draft. Recognising different national approaches the drafters of the Convention left it to the states to decide about this aspect of criminalisation.

CYBER CRIME LAW IN INDIA

The general laws in India were drafted and enacted in the 19th century. Whilst each of the general laws have undergone modifications and amendments, the broad and underlying provisions have withstood the test of time, including unimaginable advancements in technology, which speaks to the dynamism of the General laws. The general laws referred to in this Article are the Indian Penal Code, 1860 ("IPC"), which is the general penal law of India and the Indian Evidence Act,

1872 ("Evidence Act"), the general law pertaining to admissibility of evidence in civil and criminal trials. The manner in which trial of criminal cases are to be conducted is dealt with under the Criminal Procedure Code, 1973 ("Cr. P. C"). India got its first codified Act in the Information Technology Act, 2000 ("IT Act), which fell far short of the Industry's requirements to meet global standards. The focus of the IT Act was however recognition of electronic records and facilitation of e-commerce. Barely ten sections were incorporated in the IT Act to deal with Cyber Crime. At the time when the IT Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks, data theft, illegal access to data/ accessing and removal of data without the consent of the owner, etc., were listed as civil penalties under the IT Act. The IT Industry continued to rely on self-regulation and contractual undertakings to appease its global clients, as it had done before the passing of the IT Act.

The primary offences under the IT Act were:

- Tampering with source code;
- Deleting, destroying or altering any data on any computer resource with mala fide intent to cause wrongful loss or to diminish its value;
- Publishing or transmitting pornographic material through a computer resource;
- Provisions pertaining to encryption technology, the right of the Government authorities to intercept and decrypt such data and to call upon any entity or individual to decrypt such data were also included in the IT Act. Certain acts affecting the integrity and sovereignty of the nation were classified as offences.

The saving grace of the IT Act were the amendments carried out to the IPC and Evidence Act, which to some extent provided for prosecution of rampant offences like the Nigerian Scams, Phishing and other Banking frauds may be prosecuted. Cyber Crime prosecution was however not resorted to in many instances due to lack of awareness (amongst both the victims and the enforcement authorities) about the applicability of such general Laws to cyber crimes (like Phishing). To add to this,

administrative delegation of powers treated offences under the IT Act differently to those falling under general laws! Further, crimes like data theft; illegally accessing/ removal of data; virus attacks etc., could not be prosecuted due to the lack of relevant penal provisions.

S.66 of the Act misleadingly titled “hacking” is one of the most misused and abused provisions in India. Recently *i.e.*, in September 2009, the Delhi High Court has quashed the criminal proceedings initiated in or about July 2005, under S.66 of the IT Act by M/s. Parsec Technologies Ltd., against some of its former employees, who left and started their own Company, holding that the continuation of the proceedings would amount to abuse of process of law.

Likewise the IT Act did not provide sufficient recourse for women and child victims of cyber crimes like Cyber Stalking and paedophilia. Controversy has dogged the IT Act from its inception. The Ministry of Information Technology prepared and posted proposed draft amendments to the IT Act in 2005. In 2006, the IT Bill with substantial changes brought about as a result of the objections to the proposed amendments of 2005 was tabled before the Parliament. In December 2008 as a knee-jerk reaction to the November 2008 terror attacks in Mumbai, India, the Information Technology (Amendments) Act, 2008 (“ITA, 2008”) was hastily tabled before the Parliament and was passed hastily and without any debate whatsoever. Unlike the IT Act of 2000, the focus of the new ITA 2008 is clearly on Cyber Terrorism and to a significant extent, Cyber Crime. This paper deals with some important provisions of ITA, 2008 relating to data protection, privacy, encryption and cyber crime and to what extent it arms one against emerging trends in Cyber Crime.

Definitions

The replacement of the word “Digital” with the word “Electronic”, which makes the IT Act more technology neutral and expands its applicability beyond just the digital medium.

- Inclusion of cell phones, personal digital assistants and other such devices in the definition of

“Communication Devices” broadens the scope of the statute.

- The modified definition of “Intermediary” includes all service providers in respect of electronic records again broadens the applicability while inclusion of Cyber cafes in the definition of Intermediaries removes the need to interpret the statute.

The extensive definition of “cyber security” as including protection of both data and the equipment from unauthorised access, use, disclosure etc., is another vital inclusion that impacts the new Data Protection provisions included under the ITA, 2008. The relevance of these definitions, where applicable are set out below.

Data Protection

The IT industry has been lobbying for a law to protect Data and the new legislation has addressed the industry's demands to a certain extent particularly since Mphasis Limited, a Pune based Company suffered the notoriety of puncturing the Indian BPO fairy tale in April 2004, when some of its employees stole confidential credit card information of clients and used it to siphon substantial amounts. Apart from highlighting the security lapses within the Company, this case also brought to the limelight the lack of suitable Data Protection Laws in India. Several cases have now been reported where former employees are accused of data theft and misuse of Confidential and proprietary Information and data. In one instance, a BPO Company purportedly closed down due to rampant data theft.

The Indian Legislature's response to the hue and cry raised is the transposition of certain civil penalties into criminal offences and the addition of one section under civil penalties as set out hereunder:

- The only provision under the IT Act for data protection was S.43, which only imposed Civil Penalties in the event of the commission of certain acts without the permission of the owner or person in charge of the computer or computer systems such as:

- Securing access (without permission);
- Downloading or copying of data stored in a computer or computer system;
- Introducing computer viruses;
- Damaging computers and or data stored therein;
- Disrupting computers;
- Denial of access;
- Abetting such acts;
- Illegal charging for services on another's account.

S.43A has now been added under the ITA 2008 to address the data protection requirements of the Industry. S.43A stipulates that any "Body Corporate" possessing, dealing with or handling any "sensitive personal data or information" in a computer resource it owns, controls or operates, is liable for negligence, if it fails to maintain "reasonable security practices and procedures" and thereby causes wrongful loss or wrongful gain to any person. What amounts to reasonable security practices and procedures remains to be finalised by the Central Government.

Apart from the above addition under Civil Penalties, the Civil wrongs set out under S.43 of the IT Act have now been qualified as criminal offences under the ITA 2008 under S. 66. A reverse transposition has further been carried out under the ITA 2008 of two criminal provisions from the IT Act (S.66 and S.65) as civil penalties under S.43 (i) & S.43 (j), respectively. Any act set out under S.43, if committed "dishonestly or fraudulently", would amount to a criminal offence, punishable with punishment of up to three years or fine of a maximum of Rupees Five Lakhs or both, under the ITA 2008.

Though S.66 of the IT Act has purportedly been deleted, the addition of S.43 (i) under the ITA 2008 has in effect resulted in the retention of the contentious S.66 of the IT Act. However retention of S.65 of the IT Act without any modification despite its transposition into S.43 appears to be a tautology, which could be due to oversight. S.66B inserted by the ITA, 2008 is on the lines of similar provisions in the Indian Penal Code

("IPC"), which provides for punishment of the receiver of stolen property. S.66B makes the receipt or retention of a stolen computer resource or communication device punishable with imprisonment up to three years or with fine up to Rupees One Lakh or both.

Whilst S.66B may seem to also apply to hardware, which is also covered under the IPC, the term "computer resource" is defined under the IT Act as a "Computer, computer system, computer network, data, computer database or software." The extension of the above provision to the receiver of stolen data, software etc., may prove to be substantially useful when faced with issues of Corporate Espionage.

Further Analysis of the Data Protection Legislation

Although the data protection provisions introduced by the ITA, 2008 may not comprehensively address the industry specific requirements applicable to data providers and handlers; nevertheless this is an important head start towards introduction of specific data protection legislation in India, which is absolutely essential in today's business environment. One of the important outcomes of the ITA, 2008 amendments is the clarity on whether Data theft is considered a criminal offence. Commission of acts provided in S.43 to 66 dishonestly or fraudulently, clearly implies "Data Theft" as an offence in such instances.

However these acts would amount to a punishable offence only if such data is "downloaded, copied or extracted" from a computer resource. Therefore it may be argued that the provisions of S.43 (b) are not inclusive, as they do not provide for removal of data through uploading. Criminal provisions give rise to liability only in cases of unambiguity.

If a provision has to be applied through interpretation, then such interpretation, which favours the Accused, would have to be applied. With the addition of S.43A by the ITA, 2008, the onus of implementing "Reasonable Security Practices" is on the business entity. Whilst this may be a known liability that parties agree upon, unsuspecting companies or firms may get mulcted with liability if duties and obligations are not

specified, as the Central Government guidelines will then become applicable. As of now, violations under S.43 A are however not criminal offences.

Confidentiality and Privacy

India was shocked out of its complacent conservatism due to the widespread circulation of a MMS clip shot by a Delhi schoolboy. This case took an unexpected twist when this clip was circulated on Baze.com and its Chief Executive Officer of American origin was arrested. S.66E has now been introduced under the ITA, 2008 for the protection of physical or personal privacy of an individual.

This section makes intentional capturing of the images of a person's private parts without his or her consent in any medium and publishing or transmitting such images through electronic medium, a violation of such person's privacy punishable with imprisonment of up to three years or with fine up to Rupees Two Lakhs, or both. A case of posting of the personal information and obscene material on a Yahoo! Site was touted as the fastest trial and conviction of a cyber crime case in Chennai. It appears that this conviction has recently been reversed.

S.72 A of the ITA, 2008 now explicitly provides recourse against dissemination of personal information obtained without the individual's consent through an intermediary or under a services contract, with intent to cause wrongful loss or wrongful gain. The maximum punishment prescribed for this offence is three years imprisonment, or fine up to Rupees Five Lakhs or both. Service providers on the Internet, social networking sites, Companies, firms, individuals and other intermediaries ought to now be careful in the collection, retention and dissemination of personal data. Interactive websites and P2P site operators also have to be extremely careful to ensure that the provisions of S.66E and S.72 A are not violated.

Other Cyber Crimes Including Cyber Terrorism

Provisions to combat cyber frauds have now been introduced under the ITA 2008. However certain issues relating

to protection against banking frauds such as Phishing, money transfers through online hacking, e-mail frauds and cyber squatting (including through wilfully misleading domain names) to name a few have not been addressed separately in the ITA, 2008, even though these are significantly increasing problems. S.66C inserted by the ITA, 2008 makes dishonest or fraudulent use of a person's electronic signature or identity, password or any other unique identification feature punishable as theft with imprisonment of up to three years and fine up to Rupees One Lakh.

S.66D inserted by the ITA, 2008 makes cheating by personating through a computer resource punishable with imprisonment of up to three years and fine up to One Lakh Rupees. It may be noted that S.419 of IPC already provides for punishment for cheating by personating but does not provide for the maximum fine imposable. In addition to S.67 of the IT Act, S.67A and S.67B have been included by the ITA, 2008 *inter alia* to combat child pornography. S.67A makes transmission of a sexually explicit act or conduct punishable and S.67B makes publishing and transmission of child pornography an offence, punishments for which range from five to seven years and fine.

Several exceptions have also been set out to S.67 and S.67A, including for depictions in any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form. Further, S.67C introduced by the ITA, 2008 imposes liability on Intermediaries for retention and production of information. However the duration, manner and formats of retention of such information are still subject to prescription by the Central Government. This section appears to be directed mainly against Cyber Cafes and has already been subject to dissension. Failure to comply with such requirements is punishable with imprisonment up to three years and also fine.

Observations on the Cyber Crime Provisions under the ITA, 2008

- S.43 was included in the IT Act, 2000 to address certain kinds of illegal acts. However, the Legislature

has not looked beyond S.43 to address recent trends in Cyber Crimes and for dealing with such issues.

- S.66 of the IT Act, under the heading “Hacking” which was misleading was criticised for its ambiguity and for the possibility of abuse. However, whilst the proposed amendments sought for its deletion, this section has been transposed to not only being applicable as a civil penalty but is also retained as a criminal offence. With the retention of S.66 of the IT Act, one of the main issues that need to be addressed is the criminality of actions resulting in “diminishing of value” of any information residing in a computer resource. Even if the law – makers thought fit to retain this provision, its use and abuse Since, 2000 ought to have been evaluated when re-defining this provision.
- S.66C only addresses some kinds of cyber frauds and not all such frauds committed without using digital or electronic signatures. Further S.66D may be considered redundant in the light of the amendments made to the IPC after the enactment of the IT Act in 2008, save and except for the maximum fine imposable under the ITA, 2008.
- S.67A is a much – needed introduction to the IT Act and would help in combating the pernicious offences of child pornography as observed in some recent shocking incidents involving school children. Several new provisions have been introduced under the ITA 2008 to combat Cyber Terrorism. These provisions appear to be a necessary and welcome addition though there are apprehensions about their abuse and whether the Government authorities are well equipped to handle and protect the information, acquired by it in compliance with such provisions.
- S.66A inserted by the ITA, 2008 is an essential provision from the perspective of combating Cyber Terrorism and to address several instances of cyber stalking, cyber harassment, etc. However this provision can also be easily abused. S.66A provides for

punishment of three years and fine against any person found guilty of: (i) sending information through a computer resource or device, which is grossly offensive or of menacing character; (ii) false information intended to annoy, inconvenience, deceive or mislead the addressee or recipient about the origin of such message; or (iii) endanger, obstruct, insult, injure, intimidate or to cause enmity, hatred or ill will. This would not only help the police against anonymous and false messages etc., and harassed individuals, but also corporate bodies, which could rework their internal policies in consonance with this provision.

- S.66F directly addresses the issue of cyber terrorism. Acts intended to: (i) threaten the unity, integrity, security or sovereignty of India; (ii) to strike terror in the people or any section of the people by denial of access, hacking and virus attacks; and (iii) by such means does or may cause death or injuries to persons or damage to property or disrupts supplies or services essential to the life of the community; or (iv) adversely affects the critical information infrastructure; is the commission of Cyber Terrorism, the punishment for which ranges from imprisonment from three years to life and fine depending upon the seriousness of the crime.

Encryption and Data Privacy

Mid 2008, customers in India thought twice about buying Blackberry phones – no reflection on the performance of the phones but due to a sudden conflict between the Department of Telecommunications of the Indian Government (“DoT”) and Research in Motion (“RIM”) Blackberry Services. DoT requested RIM to share its encryption codes with the department, stating security concerns over data transmitted through e-mail services on Blackberry phones or to set up servers in India and permit DoT to monitor such transmissions. After several rounds of talks the Government of India dropped its request reversing its stand on the issue of a security threat.

The Indian Telegraph Act, 1885 vests extensive and absolute power on the DoT *inter alia* to deal with, monitor and regulate transmission of messages within India. These provisions therefore stand automatically extended to transmission of encrypted Data also.

The Guidelines issued by the DoT for transmission of encrypted data and the ISP license requirements permits transmission of encrypted data of 40 bit key length in RSA algorithms or its equivalent in other algorithms without having to obtain permission from the Telecom Authority. However, if encryption equipments higher than this limit are to be deployed (which would be the case for most encrypted data), individuals/groups/organizations require prior written permission of the DoT and may be further called upon to deposit the decryption key, split into two parts, with the DoT. These provisions appear to have prompted the Blackberry case. Now in addition to the above powers vested in the Telecom Authority of India, certain provisions have been added under the ITA 2008 (as set out hereunder), which further strengthens the hands of the Telecom Authority in India.

S.69 of the IT Act, which dealt with encrypted data has been replaced with a new S.69, which empowers the Central Government or a State Government through their authorised officers to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. These powers may be exercised for reasons set out in S.69 including in the interest of the sovereignty or integrity of India, defence, security of the State, or even for preventing commission of any cognizable offence or for investigation of any offence.

The only restraint in exercising such powers is the necessity of maintaining written records of such actions. The additions to S.69 and inclusion of new provisions under S.69A to S.69C under the ITA 2008 may be subject to criticism and concern. S.69A empowers the Central Government or any of its authorised officers to block or cause to be blocked access by public of any information generated, transmitted, received, stored or hosted in any computer resource. Under S.69B, the

Central Government may, through its authorised agency, monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for enhancing cyber security and for identification, analysis and prevention of intrusion or spread of virus in the country. Intermediaries have to provide such data and assistance as sought by the authorised agency and failure to extend such assistance is punishable with imprisonment up to three years and fine.

S.70A and S.70B provides for notification of any Government organization as the national nodal agency for Critical Information Infrastructure Protection and notification of any Government organization as the Indian Computer Emergency Response Team, respectively. S.84A gives extensive powers to the Central Government to prescribe encryption methods to ensure secure use of the electronic medium and for promotion of e-governance and e-commerce.

Other Relevant Provisions

S.77A of the ITA, 2008 provides for compounding of offences under this Act, other than:

- Offences punishable with life or imprisonment for a term exceeding three years;
- In cases of enhanced punishment;
- Those affecting the socio economic conditions of the country;
- Offences against a child below the age of 18 years or a woman.

Whilst some of these exceptions appear to be precise and appropriate, certain others appear ambiguous *i.e.*, exception on the grounds of socio economic conditions.

S.77B makes all offences punishable with three years and above imprisonment cognizable and bailable, notwithstanding the provisions of the Indian Code of Criminal Procedure, 1973. With the increase in cyber crimes amounting to offences under the ITA, 2008, the power to investigate offences under this Act has been vested with an Inspector instead of the Deputy Superintendent of Police. This may reduce the confusion

relating to jurisdiction for registering of offences. Further this would entail commencement of extensive and immediate cyber law awareness measures by the investigation agencies throughout India. There is however anxiety in the minds of the industry about the ability of the police official of such rank being able to handle such additional responsibility.

S.79 has been modified by the ITA, 2008 to restrict the liability of an Intermediary under this section to specific instances, *i.e.*, if he provides access to communication systems for transmission or temporary storage of third party information, data or communication links made available or hosted by him. The Intermediary should however observe due diligence and comply with the prescribed guidelines, while discharging his duties.

S.85 of the IT Act, which imputes vicarious liability in case of offences by companies, has been retained in its original form despite criticism by different industry sectors. As most of the offences under the IT Act have been made cognizable, and with the increase in the number of offences added under the ITA, 2008, this provision may be cause for concern.

Conclusion

Though the ITA 2008 has been passed by the parliament, the Amended Act is still not the law of the land. The ITA 2008 will come into effect only from the date notified by the Government of India, which still remains pending as on the date of publication of this paper.

Introduction of several provisions in the IT Act by the ITA, 2008, relating to data protection, are extremely essential in today's business environment as several Indian companies providing services to or in conjunction with foreign entities handle large amounts of data that are accessed and/or processed by their employees. Such cross border exchange/transmission of Data further mandates compliance with the provisions of foreign enactments on Data Protection. The increased accountability of data handlers and data aggregators and the enhanced punitive measures, therefore meets such requirements to some extent. The existing provisions along

with the additional/ revised provisions under the ITA, 2008 provide for criminal prosecution and stringent monetary penalties that are likely to act as effective deterrents. Whilst some inclusions in the ITA 2008 have been subject to criticism, the amendments and additions made to the IT Act are expedient and much awaited additions. Absence of effective provisions to combat offences like Cyber Stalking and cyber squatting are avoidable loopholes, which one hopes will soon be rectified. One could safely conclude that whilst the ITA 2008 is still work in progress, it is definitely headed in the right direction.

Chapter 11

Cyber Crime and Cyber Security

INTRODUCTION

The history of crime and crime prevention has been akin to the history of warfare: an Offence is developed, then a Defence counters the Offence, then a new Offence counters the new Defence. Machine guns led to the development of tanks which led to the development of rocket propelled grenades, etc. When commerce consisted of camel caravans, people in the Arabian Peninsula promoted banditry, ultimately forcing the commerce to go by sea.

When merchants used the sea lanes through the Mediterranean, the people of the Maghreb promoted the Barbary pirates until they were ultimately countered by a punitive US military action. More recently, with the advent of the railroads came Jesse James, countered by the Pinkertons and so on. Airlines discovered airline hijackers and parried the threat with the excruciating experience they call airport security.

Move followed by counter-move. In the present conditions of economic crisis with thousands of recently fired, super-computersavvy techies on the loose, the venue for those of dishonest bent is the cyber-world. The newest bandits are the malicious professional "hackers" who are not only well organised but will strike with proven military precision driven by monetary gain. Thus, businesses must learn to be en garde and protect their cyber property, such as Intellectual Property (IP), which frequently accounts for 70 per cent of the market value of companies that specialise in franchising and licensing.

The commonly accepted definition of cyber security is the protection of any computer system, software Programme, and data against unauthorised use, disclosure, transfer, modification, or destruction, whether accidental or intentional. Cyber attacks can come from internal networks, the Internet, or other private or public systems. Businesses cannot afford to be dismissive of this problem because those who don't respect, address, and counter this threat will surely become victims.

THE RISK

Cyber-crime is on the rise. On average, there has been a reported cyber security event every single day Since, 2006. If there's a transaction that involves a card with a magnetic strip and a swipe, there's a transaction that involves a risk. And if there's a computer system with software designed to allow access by multiple users (e.g. by franchisees, vendors, or other providers) without security in mind, then there's a major risk of being hacked for malicious or competitive purposes.

Mobile devices, often containing sensitive data, are lost or stolen every day. Face it: With the proliferation of free hacking tools and cheap electronic devices such as key loggers and RF Scanners, if you use e-mail or your company's systems are connected to the Internet, you're being scanned, probed, and attacked constantly.

This is also true for your vendors and supply chain partners, including payment processors. E-mail and the web are the two main attack vectors used by hackers to infiltrate corporate networks. So, clearly, every company is vulnerable because every company needs to have these functions. Conversely every company needs to guard its systems against unauthorised access through these openings because supposed firewalls offer no protection whatsoever once a hacker has entered.

WHO'S BEEN HACKED

As they say in the cyber security world, there are only two kinds of computer systems: those that have been hacked and those that will be hacked. For example, crooks used

sophisticated methods to evade detection and place malware on nearly 300 Hannaford Bros. supermarket servers to intercept payment information. As many as 4.2 million credit and debit card numbers may have been exposed. Ironically, Hannaford was notified of its massive problems on the very same day it was recertified as being Payment Card Industry Data Security Standard-compliant. *Like an AIDS test, penetration testing in the cyber security arena offers assurance and protection only as of the date of the testing.* So once is not enough.

Penetration testing must be done regularly and thoroughly to maintain its value or it becomes worth no more than a cancelled subscription. And just because people are computer savvy does not mean their data are safe. The Web site of online retailer Geeks.com featured the “hacker safe” notification from McAfee ScanAlert. Nevertheless, a hacker broke in and accessed customer credit card numbers and other personal information on its site. And in another really scary example, mortgage giant Fannie Mae narrowly avoided a software time-bomb set to destroy all data on its computers. Some disgruntled contractor who had been terminated embedded into the system a malicious code, tucked at the end of a legitimate software Programme scheduled to run each morning.

It was set to go into effect (months after he was gone) on all 4,000 of the company's servers. It was only discovered by chance by another Fannie technician or the whole agency's database would have been wiped out. Even Deborah Platt Majoras, Chairman of the Federal Trade Commission from 2004 to 2008, was a victim of identity theft.

So it's no wonder that she and the FTC have been such strong proponents of protecting consumers from shoddy data protection practices and enforcing regulations and levying fines on businesses.

WHAT COULD HAPPEN

Lots of things: all of them bad. Accordingly, a company (particularly franchise businesses and other licensors) must evaluate its risk to determine and implement appropriate policies and procedures.

We have formulated a "Chan Scale of Cyber In-Security"®, based on the potential harm that can be caused:

- *Low risk:* Hacker has gained entry to system but minimally. Minor risk of business disruption, but access can aid attackers in information gathering and planning future attacks.
- *Medium Risk:* Malware has been implanted in the company's network, which could cause malfunctions and mischief. There is a significant risk of a business disruption that could result in financial loss and/or damage of goodwill.
- *Medium-to-High Risk:* Using sniffers or other equipment, hackers have obtained personally identifiable information (PII) from point of sale (POS) systems. There is a significant risk of a business disruption that could create financial loss and/or damage of goodwill.
- *High Risk:* Inside job: data stolen by disgruntled employee. There is a potential risk of business disruption, resulting in financial loss and damage of goodwill. PII may be taken, as well as company's confidential information and financial information.
- *Critical Risk:* Hackers have gotten into the system and can access PII as well as the company's financial information and confidential information. There is a severe risk of business disruption, financial loss, damage of goodwill. System, application, and database have been compromised.

POTENTIAL LIABILITIES

Major liability may be incurred from, *inter alia*, individual litigation, class litigation, regulatory investigation, contract dispute, loss of customers, reputation damage, data theft, denial of service, cyber-terrorism, cyber-extortion, and fraud.

Some statutes impacting cyber-liability include:

- Communications Act of 1934, updated 1996
- Computer Fraud and Abuse Act of 1984
- Computer Security Act of 1987

- Economic Espionage Act of 1996
- Electronic Communications Privacy Act of 1986
- Federal Privacy Act of 1974
- Health Insurance Portability and Accountability Act of 1996
- National Information Infrastructure Protection Act of 1996
- U.S.A. Patriot Act of 2001
- Payment Card Industry Data Security Standard (PCI DSS) effective 2006 – industry-defined standard, not government

Introduced in 110th Congress (2007) – none enacted:

- Personal Data Privacy and Security Act of 2007
- Data Accountability and Trust Act
- Identity Theft Prevention Act
- Data Security Act of 2007

Introduced in 111th Congress:

- S.139, Data Breach Notification Act

POLICIES/PROCEDURES

Participants at the Davos conference on the international economy that ended in February 2009 took note of the world-wide gangs and other criminal organizations invading the cyber world. They estimated the damages from cyber crime to be \$1 trillion per year. The cost of notifying customers alone in the case of a cyber event has been estimated at \$1-3 per file accessed and \$100-300 or more per file compromised.

In light of these numbers, companies are well advised to have policies in place with respect to data protection, data retention, data destruction, privacy, and disclaimers to customers. And, if a security breach occurs, the company should expect, and be prepared for, a regulatory investigation during which the company will have to show that its policies were well documented, updated as business processes change and *observed*, or risk significant fines, agency oversight, or worse. The policies must be more than mere window dressing; failure to conform to a company's own stated, internal policies may be worse than having no policies at all. For example, the

FTC recently went after two companies for failing to provide reasonable and appropriate security for sensitive consumer information, leading to identity theft and forced a settlement containing bookkeeping and record-keeping provisions to allow the agency to monitor compliance.

Under the terms of the settlement, the FTC ordered the two companies to hire third-party security auditors to assess their security Programmes on a biennial basis *for the next 20 years*; to certify that the companies' security Programmes meet or exceed the requirements of the FTC's orders; and to prove that the companies are providing "reasonable assurance that the security of consumers' personal information is being protected."

A similarly onerous set of conditions was imposed in February 2009 by the FTC as part of a settlement with CVS Caremark, requiring that company to establish policies for protecting and properly disposing of personal information, to be subject to a biennial audit by a third party, *and to pay a multi-million dollar fine* for improper treatment of information required to be protected under HIPAA.

CYBER CRISIS PLANNING/MANAGEMENT

IT (Information Technology) systems are vulnerable to a variety of disruptions from a variety of sources such as natural disasters, human error, and hacker attacks. These disruptions can range from mild (e.g. short-term power outage, hard disk drive failure) to severe (e.g. equipment destruction, fire, online database hacked).

Crisis (and Disaster Recovery) planning refers to those interim measures needed to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods to minimise the business impact. In January 2009 Heartland Payment Systems, which processes 100 million credit and debit card transactions per month, disclosed that hackers had

penetrated its computer network. By installing malicious software, the hackers gained access to digital information encoded on a card's magnetic strip that could be used to create duplicate cards. In the wake of what was described as the biggest single breach of consumer and financial data security ever, Heartland's stock was hit hard. In public statements following the incident, Heartland's CEO compared the potential industry-wide impact of the breach to the Tylenol poisonings that nearly brought down the drug maker Johnson & Johnson in the early 1980s. The Heartland debacle highlights the potential fallout companies face as a result of ineffective planning for data security breaches. The costly consequences may include damage to reputation and brand value, shareholder derivative suits, directors' and officers' liability, regulatory agency investigations, and class-action litigation. Effective crisis planning and crisis management processes must be developed to enable businesses to continue operating following failure of, or damage to, vital services or facilities.

The cyber crisis planning process covers the following:

- The technology that supports them (servers, databases, applications) and technology owners.
- Identification and agreement with respect to all responsibilities and emergency arrangements for business continuity planning and recovery with all affected parties throughout the organization.
- 'Call Tree' and contact details.
- Documentation of workarounds (electronic and manual) and/or rectification procedures and a linkage to any relevant reference material or documents.
- Appropriate education of staff in the execution of the agreed emergency procedures and processes.
- Checklists and procedure guidelines to assist all parties to recover from a crisis or disaster.
- Testing and updating of the plans on a regular basis.

Cyber Crisis Management (Incident Response – Stop the bleeding) process covers the following:

- *Identify the Crisis at Hand:* For example, is it a customer data breach, privacy breach, virus outbreak,

targeted malicious code attack, denial of service attack, phishing attack, or third party data compromise?

- *Analysis and Assessment:* Triage of the incident to determine the severity and impact on the business.
- *Coordination/Response Plan:* Decide whether to protect or prosecute including contacting the proper law enforcement authorities. If prosecution is the course of action, all evidence (system/application logs, audit trails, and affected systems) must be collected in a forensically sound manner to hold up in a court of law. Contact all affected parties and communicate and agree upon a response plan.
- *Containment/Recovery Plan:* Restore affected systems to normal business operation.
- *Incident Learning:* What can be learned from this incident? What can be improved so this type of incident does not again?

REGULAR SURVEILLANCE

Many companies overlook the fact that security monitoring or surveillance is necessary in order to protect their information assets. Security Information Management Systems (SIM), if configured properly, can be useful in collecting and correlating security data (system logs, firewall logs, anti-virus logs, user profiles, physical access logs, etc.) to help identify internal threats and external threats.

A successful surveillance Programme includes practices such as:

- Security in Depth is a best practice. Several layers of security are better than one. Surveillance on each layer of security will help identify the severity of a security event; alerts coming from the internal corporate network might be more urgent than on the external network.
- Critical business data should be encrypted with strict role-based access controls and logging of all changes for an accurate audit trail.
- A policy of “least privileges access” should always be

implemented with respect to sensitive information and logs should be reviewed regularly for suspicious activity.

- Review of Identity Management Process to determine who has access to what information on the corporate network. Ensure that the access of ex-employees, contractors and vendors is eliminated when they are no longer needed or leave the organization.
- Placement of Network Intrusion Detection/Prevention Systems throughout the corporate network to help detect suspicious or malicious activity.

ACCESS CONTROLS

Curiosity is a natural human trait. The viewing of private records of political figures and celebrities has led to people losing their jobs or being criminally convicted.

Most of these workplace incidents were not tied to identity theft or other bad intentions, but were simply instances of employees taking advantage of access control policy gaps, sometimes without realising that they were breaking privacy laws and exposing their organizations to risk. So companies need to focus on ensuring that employees' access to information is required for their particular job.

Sometimes employees' access is supplemented as they are promoted, transferred, or temporarily assigned to another department within the organization.

Users that drag such excess access into their new role may create holes in corporate security or create other business risks. These are common problems in large organizations, a natural consequence of the pressure on IT departments to provide access quickly when employees are transferred or promoted.

Organizations should consider putting automated controls in place for cyber-access to ensure that user privileges are appropriate to their particular job function or process role. Access to personally identifiable information must be governed by the need; there must be a valid business reason for access.

The human factor is the weakest link in any information security Programme. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime.

Below are a few best practices:

- Use a “passphrase” that is easy to remember — E@tUrVegg1e\$ (Eat your veggies) and make sure to use a combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks. Try not to use simple dictionary words as they are subject to dictionary attacks – a type of brute force attack.
- Do not share or write down any “passphrases.”
- Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.
- Do not click on links or attachments in e-mail from untrusted sources.
- Do not send sensitive business files to personal e-mail addresses.
- Have suspicious/malicious activity reported to security personnel immediately.
- Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.
- Educate employees about phishing attacks and how to report fraudulent activity.

CONCLUSION

The risks of cyber crime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it.

At the very least, every company must conduct a professional analysis of their cyber security and cyber risk;

engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thoughtout cyber policy, including crisis management in the event of a worst case scenario.

Chapter 12

Cyber Crime in India

The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines.

Internet has enabled the use of Web site communication, e-mail and a lot of any time anywhere IT solutions for the betterment of human kind. Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material.

This includes not only educational and informative material but also information that might be undesirable or anti-social. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-hackers, to Internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities.

Increase in cyber crime rate has been documented in the news media. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

TRADITIONAL CRIME

Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual property. Cyber crime in the context of national security may involve hacktivism, traditional espionage, or information warfare and related activities. Cyber crimes have been reported across the world. Cyber crime is now amongst the most important revenue sectors for global organized crime, says Frost and Sullivan Industry Analyst Katie Gotzen.

Because of this, the potential risks associated with malware have risen dramatically. Unlike in traditional crimes, the Information Technology infrastructure is not only used to commit the crime but very often is itself the target of the crime. Pornography, threatening e-mail, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime. There are two sides to cyber crime. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that, the number of cyber crimes committed

should be related to the number of victimizations experienced. Of course there will not be a one-to-one correspondence since one crime may, inflict multiple victimizations multiple crimes may be responsible for a single victimization. Some crimes may not result in any victimization, or at least in any measurable or identifiable victimization. The obvious effect of cyber crime on business is the evolving threat landscape. 'The motive of the attacks has changed over time. Earlier, the intent of the attacker was to gain fame although the motivation was criminal. Cyber crime economics are too compelling to subside.

CYBER CRIME VARIANTS

There are a good number of cyber crime variants. A few varieties are discussed for the purpose of completion. This article is not intended to expose all the variants. The readers are directed to other resources.

Cyber Stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening Behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorised access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.

Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account

for some reason. Customers are directed to a fraudulent replica of the original institution's Web site when they click on the links on the e-mail to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. F-Secure Corporation's summary of 'data security' threats during the first half of 2007 has revealed that the study found the banking industry as soft target for phishing scams in India.

Cross-site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

Cyber Squatting

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000. Bot Networks A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of

computers without the users realising it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal.

Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor' is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed Programme, or could be a modification to a legitimate Programme. Bot networks create unique problems for organisations because they can be remotely upgraded with new exploits very quickly, and this could help attackers pre-empt security efforts.

VULNERABILITY

The Open-Source Vulnerability Database (OSVDB) project maintains a master list of computer - security vulnerabilities, freely available for use by security professionals and projects around the world. Vulnerability information is critical for the protection of information systems everywhere: in enterprises and other organizations, on private networks and intranets, and on the public Internet.

INDIAN CRIME SCENE

The major cyber crimes reported, in India, are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. Given the fact that nearly \$ 120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of

information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

Phishing

Phishing attacks were more popular among Indian users due to rising Internet penetration and growing online transactions. India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card details. A non-resident Malayali, had an account in a nationalised bank in Adoor, lost \$ 10,000 when the bank authorities heeded a fake e-mail request to transfer the amount to an account in Ghana.

In Mangalapuram, a person transferred a large sum of money as "processing charge" to a foreign bank account after he received an e-mail, which said he had won a lottery [Kerala: The Hindu Monday Oct 30 2006]. Reports of phishing targeted at customers of banks appear to be on the rise. Web sense Security Labs, in a statement released recently, said it had received reports of such attacks from customers of AXIS Bank.

The Economic Offences Wing (EOW), Crime Branch, Delhi Police, unearthed a major phishing scam involving fake emails and websites of UTI Bank, An analysis of the accounts of the four arrested Nigerian nationals indicated financial transactions of over ` 1 crore in an eight-month period till December 2006. Investigations revealed that the scam is multi-layered with pan-India and international characteristics The Lab went on to say that it found a mal ware in the Web site of Syndicate Bank. The users through a spoofed e-mail were asked to renew certain services and claiming that failure to do so

would result in suspension or deletion of the account. The e-mail provided a link to a malicious site that attempted to capture the personal and account information. Phishing emails have increased by approximately twenty five percent over the last year but are harder to detect as they increasingly trick unsuspecting people with ordinary scenarios instead of improbable ones such as sudden cash windfalls.

It has been six months since the phishing attack on ICICI bank customers became public, and during that period, two more such attacks were reported on customers of financial institutions in India, one of UTI Bank and the other. State Bank of India. RSA's 24/7 Anti-Fraud Command Centre of AFCC has just uncovered a 'Universal man-in-the middle Phishing Kit' in online forums which helps quickly create the fraudulent websites, often borrowing code from the original site.

Cyber Cafes—E-mails

Cyber cafes have emerged as hot spots for cyber crimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. The mushrooming of cyber cafes in the city, which provide the secrecy through cabins constructed for users, has also made the porn literature easily accessible to the people visiting them. A 23- year-old person from Tiruchi was arrested by the City Cyber Crime police on Thursday on charges of sending an e-mail threat to the Chief Minister and his family.

In another case, the police team investigating the e-mail threat on the lives of the President and the Prime Minister has prepared a sketch of the suspect, who had sent the e-mail from a cyber cafe in the city. The Case of The State of Tamil Nadu vs Suhas Katti is notable for the fact that the conviction was achieved successfully.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the

message resulted in annoying phone calls to the lady. A travel agent was arrested for allegedly sending a threatening mail to blow up the National and Bombay stock exchanges in Kolkata.

Stalking

A tenth standard boy from Bangalore got into trouble when a girl much older than him started stalking him. She pasted 'I Love You' slips on his gate and called him. On reviewing his Orkut profile, it was realised that he had accepted chat invites from more than 20 people; only two of who were his real-life friends.

Hacking

A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light. After getting the addresses, letters were sent through post mail and the recipients were lured into participating in an international lottery that had Australian \$ 23 lakhs at stake. Computer hackers have also got into the Bhabha Atomic Research Centre (BARC) computer and pulled out important data. Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward revision to some students in return for a hefty payment. A key finding of the Economic Crime Survey 2006 of Price water house Coopers (PwC) was that a typical perpetrator of economic crime in India was male (almost 100 per cent), a graduate or undergraduate and 31-50 years of age. Further, over one-third of the frauds in the country were perpetrated by insiders and over 37 per cent of them were in senior managerial positions.

GLOBAL ANTI-MALWARE MARKET

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or Programme code. The global anti-malware market is driven by cyber criminal threats. The commercialisation of

cyber crime is spurring malware-writing activity and leading to more threats of this nature. In the consumer space, this translates into identity theft and stolen passwords. Growth opportunities have led to intensified competition in both consumer and enterprise segments.

On the other hand, loss of intellectual property and customer data coupled with extortion with the threat of taking down Web sites or revealing sensitive information are on the rise in the enterprise space. Organised crime is now employing KGB-style tactics to ensnare the next generation of hackers and malware authors. Cyber-criminals are actively approaching students and graduates of IT technology courses to recruit a fresh wealth of cyber skill to their ranks. Today's worms are the handiwork of malcontents for whom cyber crime affords lucrative returns. A flourishing market exists where large blocks of infected machines that can be controlled remotely are for sale.

So big demonstrated the close nexus between malware writers and spammers, machines infected by the Sobig mass mailing worm were offered to spammers for price. The thriving market for subverted PCs has swung the underworld into hyperactivity. The past ten months have seen several hacker groups and cyber crime syndicates setting up attack networks (botnets) and releasing remote attack tools through increasingly crafty malware such as Blaster, Sinit, MyDoom, Phatbot, Bagle and Netsky. New analysis from Frost and Sullivan, World Anti-Malware Products Markets, finds that the world market for antivirus solutions reached \$4,685 million in 2006, up 17.1 per cent from \$4,000.7 million in the previous year and expects this market to grow at a 10.9 per cent compound annual growth rate (CAGR) from 2006 to 2013, reaching \$9,689.7 million by 2013.

ANTI-CYBER CRIME INITIATIVES

In a first of its kind initiative in India to tackle cyber crime, police have taken the initiative to keep an electronic eye on the users of the various cyber cafes spread over the city. The Kerala State IT Mission has launched a Web portal and a call

centre to tackle cyber crime. The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber cafe owners. Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organisations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats. Policy initiatives on cyber crime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. Prateek Bhargava, cyber law expert says, "There is huge potential for damage to national security through cyber attacks. The Internet is a means for money laundering and funding terrorist attacks in an organised manner. In the words of Pavan Duggal, Supreme Court Lawyer, "Cyber crime is omnipresent and although cyber crime cells have been set up in major cities, most cases remain unreported due to lack of awareness."

CONCLUSION

Net surfing by youngsters lures them into dangerous domain. The need for a conscious effort to checkmate the undesirable fallout of youngsters accessing and using the Internet is of concern. The print media has a duty to educate unwary parents and youngsters about the dangers inherent in treading dangerous areas in the cyber-world. Cyber Space Security Management has already become an important component of National Security Management, Military related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in cyberspace. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat. It is, therefore, necessary to put in place a 'National Cyber Space Security Management Policy' to define the tasks, specify

responsibilities of individual agencies with an integrated architecture. It is a well-known fact that terrorists have been using the Internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have the capability to paralyse large parts of communication networks, cause financial meltdown and unrest. The degree of our preparedness in the face of all these potential threats, does leaves much to be desired. The Government should also take note of this slow but worrying development and put in place a proper mechanism to curb the misuse.