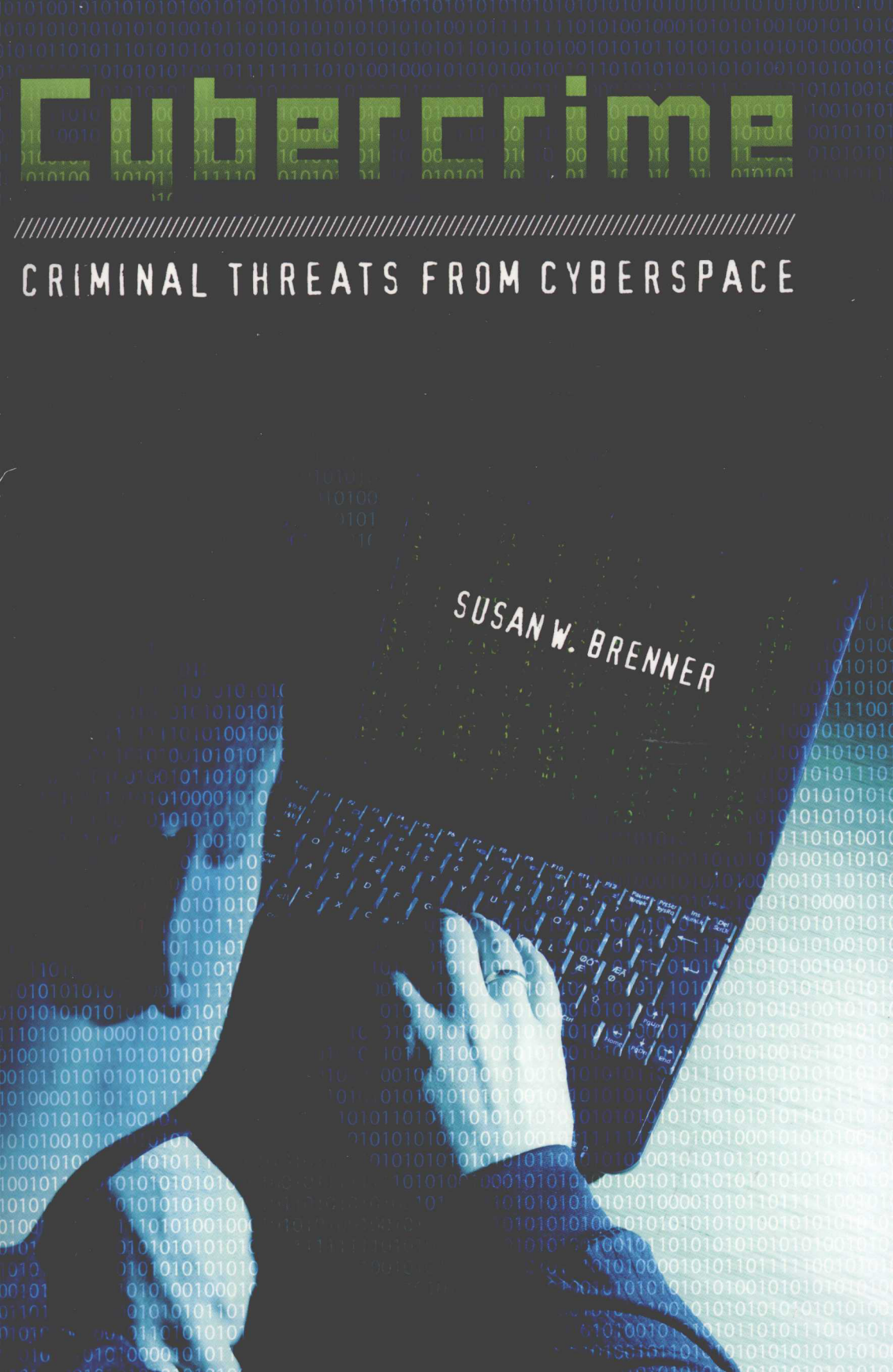


Cybercrime

CRIMINAL THREATS FROM CYBERSPACE

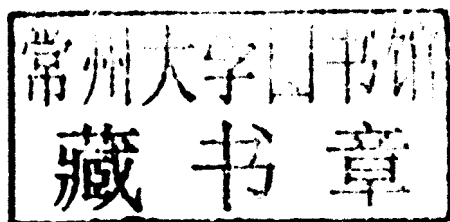
SUSAN W. BRENNER



Cybercrime

Criminal Threats from Cyberspace

Susan W. Brenner



Crime, Media, and Popular Culture
Frankie Y. Bailey and Steven Chermak, Series Editors

 **PRAEGER**

AN IMPRINT OF ABC-CLIO, LLC
Santa Barbara, California • Denver, Colorado • Oxford, England

Copyright 2010 by Susan W. Brenner

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except for the inclusion of brief quotations in a review, without prior permission in writing from the publisher.

Library of Congress Cataloging-in-Publication Data

Brenner, Susan W., 1947–

Cybercrime : criminal threats from cyberspace / Susan W. Brenner.

p. cm. — (Crime, media, and popular culture)

Includes bibliographical references and index.

ISBN 978–0–313–36546–1 (hard copy : alk. paper) — ISBN 978–0–313–36547–8 (ebook)

1. Computer crimes. 2. Computer networks—Law and legislation. I. Title.

HV6773.B75 2010

364.16'8—dc22 2009048693

ISBN: 978–0–313–36546–1

EISBN: 978–0–313–36547–8

14 13 12 11 10 1 2 3 4 5

This book is also available on the World Wide Web as an eBook.

Visit www.abc-clio.com for details.


Praeger

An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC

130 Cremona Drive, P.O. Box 1911

Santa Barbara, California 93116-1911

This book is printed on acid-free paper 

Manufactured in the United States of America

Series Foreword

This book is an outstanding contribution to the interdisciplinary series on *Crime, Media, and Popular Culture* from Praeger Publishers. Because of the pervasiveness of media in our lives and the salience of crime and criminal justice issues, we feel it is especially important to provide a home for scholars who are engaged in innovative and thoughtful research on important crime and mass media issues. It seemed essential to include a book in the series that examined the dynamic nature of cybercrime.

Many of us have a limited knowledge of the crimes that occur in the world of computers and the Internet, known as “cybercrimes” because they occur in “cyberspace.” These crimes run the gambit from scams and fraud to stalking and even terrorism. These crimes have the potential for extraordinary impact on the lives of individuals and on society as a whole. Although many people fear street crimes involving face-to-face interactions with violent strangers, they are unaware of the predatory possibilities of an e-mail solicitation.

Cybercrime is not an altogether new breed of crime. As Professor Brenner explains in this book, the crimes carried out by this new breed of criminal often reflect emotions as old as humankind. These emotions include greed, obsession, or a desire for revenge. What is new is the space in which the crimes are played out. The cybercriminal and his or her victim may be only miles apart or a world away from each other. Scam artists on another continent can seduce those inclined to avarice into parting with their money. An

obsessed acquaintance can go into cyberspace and stalk the object of his or her desire. Another can seek revenge by assuming the identity of the victim to post photos on a porn site or leave angry or embarrassing messages about the victim on another site. And it can all be done while the cybercriminal sits at his or her computer.

Cybercrime raises issues of privacy, or rather, the increasing loss of privacy. The use of the computer for legitimate activities—from banking and social networking to searches for employment—is a commonplace, almost taken-for-granted aspect of modern life. However, the information that we send into cyberspace makes us vulnerable to cybercrime. The details of our identities and our activities, once shared online, become accessible to those who would steal and misuse the information.

From the beginning, as Professor Brenner discusses, cyberspace attracted “hackers,” a breed of outlaw computer whizzes who attacked sites, such as federal agencies, to prove that it could be done. These young outlaws sometimes were recruited to develop ways of protecting the sites they had penetrated. In recent years, for professional criminals who hack into sites, it has been done for the money that can be made from crimes such as corporate extortion. The lack of a sufficient number of law enforcement and security experts trained in detecting and eradicating cybercrime means that organizations and agencies remain at risk from cyberattacks.

The goal for agencies such as the Federal Bureau of Investigation (FBI) is to reduce, if not eliminate, this risk by capturing the criminals. However, the techniques that have been developed to prevent computer intrusions frequently lag behind the ability of cybercriminals to develop a new virus or to carry on their activities beyond the reach of the U.S. government. The increased risk post-9/11 of a terrorist attack launched in cyberspace is no longer the stuff of science fiction.

At the same time, there are some issues, such as invasion of privacy of suspects or the censorship of free speech concerns, with which we must deal. At what point would such concerns be suspended in pursuit of the cybercriminal?

In this book, Professor Brenner provides an accessible and informative exploration of the history of cybercrime, the various categories of cybercrime, and the law enforcement response. Drawing on true cases of cybercrime and fictional depictions in popular culture, Professor Brenner tells us what we need to know about the new world created by the expansion of computer technology. As she illustrates, although there are reasons for concern about

cyberspace, we can only go forward into this brave new world. As the technology evolves, the responses of both citizens and the criminal justice system must also evolve.

Frankie Y. Bailey and Steven Chermak,
Series Editors

Contents

Series Foreword	vii
Chapter 1. Twenty-First Century <i>Twilight Zone</i> : Stalking a Town	1
Chapter 2. From Mainframes to Metaverse: The Origins and Evolution of Cybercrime	9
Chapter 3. Three Categories of Cybercrime	39
Chapter 4. Target Cybercrimes: Hacking, Malware, and Distributed Denial of Service Attacks	49
Chapter 5. Tool Cybercrimes: Fraud, Harassment . . . Murder?	73
Chapter 6. Cyber- <i>CSI</i> : Computer Crime Scene	103
Chapter 7. Beyond <i>War Games</i> : Who Are the Cybercriminals?	121
Chapter 8. Cyber- <i>Law and Order</i> : Investigating and Prosecuting Cybercrime	135

Chapter 9. U.S. Law Enforcement: Agencies and Challenges	149
Chapter 10. Global Law Enforcement: Few Agencies, Even More Challenges	163
Chapter 11. Privacy versus Security: Which Trumps?	177
Chapter 12. New Ways to Fight Cybercrime	207
Notes	221
Index	271

Twenty-First Century *Twilight Zone*: Stalking a Town

INTRODUCTION

In the *Twilight Zone* episode “The Monsters Are Due on Maple Street,” aliens from another planet manipulate the residents of a sleepy Midwestern suburb into turning on each other in what becomes an orgy of violence.¹ The aliens do this by turning the suburbanites’ technology against them on a summer evening. They begin by shutting off phone and electric service to the suburb.

As the residents gather in the street to speculate about what is happening, one of them named Pete leaves, saying he will walk to the next suburb and find out what “is going on.” Those left behind speculate about the outages and the odd things that preceded them: a flash of light, something passing overhead, and a loud roar. A man named Les tries unsuccessfully to start his car. As he walks away from the vehicle, the aliens start it remotely, with no one inside. This causes the other, already unnerved residents to think Les must be “in on” whatever is happening to them. They begin to interrogate Les about why he spends nights in his backyard, looking up at the sky. A boy who reads science fiction says the mysterious events are part of an invasion by “space aliens,” some of whom would have infiltrated the suburb disguised as humans. By now, night has fallen, and the residents still have no electricity, no transportation, and no communication.

Les says he is an insomniac and goes to the backyard when he cannot sleep. As he tries to explain his behavior, the lights go on in his home and loud music blares from inside. The others become even more suspicious. A neighbor named Steve tries to defend Les, which makes the crowd also suspect him of being involved in whatever is happening to them. Charlie, a loud and aggressive resident, begins cross-examining Steve about a mysterious radio he claims to be building but no one has seen. At that point, the terrified crowd sees a silhouetted figure—maybe a “space monster”—walking toward them. Frightened, like the others, Charlie grabs a shotgun and shoots at the figure, killing Pete, who had walked to the next suburb to find out what was going on.

As Charlie claims it was self-defense, the lights come on in his house, and the crowd turns on him. He runs for home, with the others chasing him and throwing stones. After being hit by a stone, he stops and tries to deflect the crowd by blaming the boy who told them an invasion was coming. (“How did he know?”) As the crowd turns on the boy, lights and telephones start going on and off in other houses, and cars and lawn mowers begin to start and stop for no apparent reason. The residents of Maple Street descend into madness, smashing windows and attacking each other.

The scene shifts to a hillside overlooking the suburb. Two aliens stand by their spaceship, watching the riot on Maple Street. One of them notes how easy it is to turn humans against each other by tinkering with the technology on which they rely.

When this *Twilight Zone* episode aired in 1960, the only entities that could have implemented the scenario it depicts were the utility companies . . . and, perhaps, space aliens. That is no longer true. As we will see in this chapter and in succeeding chapters, our ability to use cyberspace alters the fabric of our lives in fundamental and irreversible ways. The most significant aspect of cyberspace for our purposes is that our access to it erodes the monopolization of power by governments and corporations.

In 1960, only the electric company would have been able to turn the power on and off on Maple Street, and only the telephone company could have done the same with the phone service. Back then, utility companies (and government agencies, banks, and other private entities) were the masters of their respective domains. Someone bent on harassing the residents of Maple Street could have shut off the phone or electric service by cutting cables but would not have been able to tinker with the services, turning them on and off selectively. In 1960, the world revolved around tangible assets and resources; utility companies and other public and private entities could secure their assets and their processes behind walls, fences, and doors. They

could screen and limit those who had access to the premises and the assets they protected. They could, in sum, keep the rest of us, including “the bad guys,” out.

Almost 50 years later, that has changed. Walls, fences, and doors still keep people from physically invading protected places, but physical access is no longer the only option. Today, people with sophisticated computer expertise—commonly known as “hackers”—could replicate the tactics the aliens used on Maple Street except, perhaps, for remotely turning cars and lawn mowers on and off. As we will see in later chapters, cyberspace makes what used to be physically secured areas accessible to anyone with the requisite, often minimal, level of computer expertise. As a result, we effectively live in a world with four dimensions (five if you include time): the height, length, and width of real space plus virtual space. Virtual space lets those of us who are law-abiding citizens do marvelous things. Unfortunately, as we shall see, it also lets those of us who are less law-abiding break rules and wreak havoc in various ways.

Perhaps no case better illustrates the power cyberspace gives us to wreak havoc in new and terrifying ways than a 1999 incident in which a man effectively replicated the aliens’ manipulation of the hapless residents of Maple Street.

STALKING A TOWN

Townsend is a small town in northern Massachusetts, located about 55 miles from Boston. Townsend was incorporated in 1732 and had 9,501 citizens by 2000. It has four schools: a high school, a middle school, an elementary school, and a preschool. The middle school—Hawthorne Brooke—has approximately 600 students in grades six through eight and 60 faculty and staff members.

In the fall of 1999, some Hawthorne Brooke eighth-graders were spending time after school in an online chat room for Limp Bizkit fans.² They used the room to talk about personal things, as well as the band. At one point, a new person who said he was a Hawthorne Brooke student began hanging out in the chat room. Because he was from Hawthorne Brooke, the others invited him to join them in their private chat room. He did and soon was always there, ready to talk to the others and hear about how their days had gone, what was happening at home, whom they liked, and whom they didn’t . . . all the things children of that age talk about.

The new person began to say and do strange things. He said he was a serial rapist and would be coming for them. And he sent them to child

pornography that was posted online, which included horrific images of a five-year-old girl being raped. When the others pressed him to tell them who he was, he said he was an eighth-grader they talked about in the chat room. The others retaliated by harassing the innocent boy at school.

By October, the students were beginning to wonder if he really was a Hawthorne Brooke eighth-grader, both because of his increasing erratic behavior and because he was making mistakes when he talked about the school. Some of them finally told him they didn't believe he was a student at their school, which seemed to infuriate him. He said he was going to blow up their school because they didn't believe him.

On October 19, he sent them a link to a Web site with photos posted on it. One was an image of Hawthorne Brooke Middle School with the cross hairs of a rifle scope superimposed on it. Another was a photograph of the school principal, altered to make it look as if he was bleeding from bullet holes in his head and chest. The site also lauded the high-school students who had carried out the Columbine school shootings five months earlier. On October 20, the mystery person added a "hit list" to the site. It listed the first names of 24 Hawthorne Brooke students and the last names of three teachers. Under the list was this sentence: "You lucky individuals will go home with more holes in your body than you came with."

The students were terrified. When they told their parents what was going on and showed them the site, the parents were terrified, too. No one knew what to do, and no one knew whom to trust. It was clear that the mysterious person in the chat room was a local because he knew so much about what had gone on in the school from day to day—who wore what, who sat with whom at lunch, who was mad at whom, and so on.

Police and school officials held a meeting with the parents of the students whose names were on the "hit list," but no one really knew what to do about the person who posted it. Panic set in as the community realized they were at the apparent mercy of an unknown psychopath. As a member of the community noted later, their tormentor made it seem that violence was imminent, and in a post-Columbine world, everyone—students, teachers, and parents—was terrified and suspicious of each other. Everyone knew the person responsible *had* to be someone affiliated with the school; otherwise, how could he know so much about it? So students suspected their teachers, the staff at the school, and each other; parents suspected teachers, staff members, and every child but their own; and teachers and staff members suspected each other and their students. The climate must have been unimaginable.

The morning after the meeting, police used bomb-sniffing dogs to search the halls and classrooms at Hawthorne Brooke. They found nothing. They

assigned an officer to the school, to be on the lookout for . . . whatever. As students arrived, teachers searched their book bags, looking for weapons or anything suspicious—anything that might identify the person who was responsible for all of this. Many parents simply refused to send their children to school, and some teachers quit.

At that point, their mysterious tormentor took things offline and into the real world. The mother of a girl who was on the “hit list” was a secretary at Hawthorne Brooke. When she answered a call to the school, all she heard was music. Police later identified it as a song linked to the Columbine shootings. When the woman got home, the same music had been left on the family’s answering machine. Her husband was so upset he went to his brother to borrow a gun to protect his family from the person who was terrorizing their town. His brother talked him out of it.

When it seemed as if disaster would strike at any minute, the police got a break. Working with the state police, Townsend officers traced the mysterious person’s Internet activity to the Maple Woods Community College in Missouri. They later traced the calls to the school and the family’s answering machine to a pay phone at the same college. At that point, the police assumed the perpetrator was in Townsend and was working with someone in Missouri to make it seem that the online activity and calls were coming from there.

As the Massachusetts officers worked with their Missouri counterparts, it began to become apparent that their perpetrator was not, and had never been, in Townsend. The mysterious figure who terrorized a town and turned neighbor against neighbor was a 19-year-old paraplegic from Smithville, Missouri: Christian Hunold.³

Hunold’s mother was the chief financial officer for a local school district; his father was a retired high-school teacher. Until he was 15 years old, Hunold was an honor-roll student who played soccer and participated in his school band. When he was 15, he took a ride with a friend who had just gotten his driver’s license. They were on their way to a mall when the driver lost control of the car, and it smashed into a tree. Hunold was badly injured. He eventually regained the use of his arms and some use of his hands, but he would never walk again.

As the years passed and Hunold graduated from high school, his parents and friends all thought he had put the accident behind him, but he had not. He resented being physically dependent on his parents; and he seethed about the unfairness of having lost everything—sports, music, the ability to lead a regular life—while the person who was responsible for the accident, the driver, walked away essentially unharmed.

Isolated at home in his wheelchair, Hunold discovered he was good at computer programming and Web design, and he decided to study computer science at a community college. As he spent hours on the family computer, he discovered something else: He could be a different person—a strong, whole person—in cyberspace. By the time he found his way into the Limp Bizkit chat room and met the Hawthorne Brooke students, he was spending eight hours a day online, escaping the life he hated.

As Hunold got to know the Hawthorne Brooke students, he found he hated their childish obsessions and complaints, and he decided to give them a taste of “the real world.” He later told investigators he was able to pass as a Hawthorne Brooke student for so long because he spent a lot of time listening to the students talk to each other and talking to them individually. When he chatted with students, Hunold would ask about their families, their houses, their pets, and who they hung out with at lunch and other times. Thus, he acquired the information he used to convince them he was one of their classmates. As Hunold grew adept, he could chat knowledgeably about who lived where or wore what or had a dog (and what the dog’s name was). He could even chat about who sat with whom at lunch and what someone wore to school that day. One thing that made his pretense so successful was that he dealt with children, who tend to be more gullible than adults.

Hunold said he began threatening the Hawthorne Brooke students when he began to lose control of the charade—when they began to doubt that he was a student at their school. When interviewed at his home in Missouri by two Massachusetts officers, Hunold seems to have vacillated between expressing remorse and dismissing the affair as a joke. He told the officers he never had any intention of going to Townsend to carry out the threats he made and probably would not have been physically able to do so, in any event.

Perhaps the most chilling thing that came out of the officers’ visit to the Hunold home was a discovery they made when they searched the computer he used to terrorize the people of Townsend. On it, they found evidence they believed indicated that he was preparing to stalk another school—in Georgia, this time. If he not been caught when he was, Hunold might have gone on to stalk the Georgia school and other schools in other states. If he had continued, he probably would have been much better, more believable, and more terrifying the second time and with each succeeding iteration.⁴

If Hunold had been more sophisticated in his use of cyberspace, his career as a stalker of schools might not have been interrupted, at least not until after he terrorized more communities. If he had hidden his tracks—if he had made it appear he was using a computer in Massachusetts or Ohio or California—he probably would not have been caught, especially in 1999.

Cybercrime was a very new phenomenon then, and few law enforcement agencies were adept at investigating it. The Massachusetts investigators were able to track Hunold because the state had a computer crimes unit and because he apparently made no effort to hide his tracks, either when he was online or when he called the school.

The Hunold case is old news now. Cybercriminals have moved far beyond the relatively simple tactics he used to carry out his crime. But what Hunold did still perfectly exemplifies the distinctive aspects of cybercrime: A crippled boy was able to manipulate and terrorize people in a town 1,000 miles away. His use of virtual space gave him abilities no one has in the real world, where we are subject to the laws of gravity and the rules of physics. In the next four chapters, we will see how these virtual-space abilities create new crimes and alter traditional crimes. In Chapters 8 through 10, we will see how they create major challenges for law enforcement officers and, in so doing, erode the likelihood that clever cybercriminals will be caught and punished.

From Mainframes to Metaverse: The Origins and Evolution of Cybercrime

In this chapter, we trace the evolution of modern cybercrime as a new type of criminal activity. We will touch on the legal issues cybercrime raises but will examine them in detail in Chapters 3 through 5.

WHAT IS CYBERCRIME?

Before we can trace the evolution of cybercrime, we need to define what it is. More precisely, we need to distinguish “cybercrime” from “crime.”¹

“Crime” consists of engaging in conduct that has been outlawed by a society because it threatens the society’s ability to maintain order. Order cannot exist without rules that proscribe certain “harmful” activities and institutions that enforce these rules. These rules constitute a society’s criminal law. Criminal law is designed to prevent the members of a society from preying on each other in ways that undermine order. It does this by defining certain types of behavior as intolerable as “crimes.”

Crimes take many forms because each targets a specific “harm.” Crimes target harming individuals (murder, rape), property (arson, theft), government (obstructing justice, treason), and morality (obscenity, gambling).