VIOLENCE GOES TO THE INTERNET

ABOUT THE AUTHOR

Evan M. Axelrod, Psy.D. is a Police Psychologist from the Denver Metro area. He received a doctorate in clinical psychology, with an emphasis in behavioral forensics, from the University of Denver. Dr. Axelrod, a board- certified expert in traumatic stress, has been an associate with Nicoletti-Flater Associates, a company specializing in public safety psychology, trauma, and violence prevention/intervention, since June 2000. Dr. Axelrod is also an adjunct professor at the University of Denver Graduate School of Professional Psychology. Dr. Axelrod specializes in preemployment screening and is an experienced provider of therapeutic and crisis-related services to a wide range of populations. Dr. Axelrod provides training and consulting services to organizations throughout Colorado and internationally in locales such as Antarctica. Dr. Axelrod regularly conducts both direct and indirect risk assessments and fitness-for-duty evaluations and was previously involved in a project with the Colorado Bar Association that aimed to educate corporations about domestic violence.

VIOLENCE GOES TO THE INTERNET

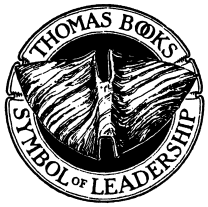
Avoiding the Snare of the Net

By

EVAN M. AXELROD, Psy.D.

With a Contribution by

John Nicoletti, Ph.D.



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 978-0-398-07881-2 (hard)
ISBN 978-0-398-07882-9 (paper)

Library of Congress Catalog Card Number: 2009006912

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
CR-R-3

Library of Congress Cataloging-in-Publication Data

Axelrod, Evan M.
Violence goes to the internet : avoiding the snare of the net / by Evan M. Axelrod ; with a contribution by John Nicoletti.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-398-07881-2 (hard) -- ISBN 978-0-398-07882-9 (pbk.)
1. Internet--Social aspects. I. Title.

HM851.A97 2009
004.67'8--dc22

2009006912

For Michelle, J.T., and Sam. Your love and support drives me and inspires me to be the best version of myself.

In memory of Nani, who will always be loved and missed.

PREFACE

As is true in any community, the Internet has a light, safe side and a dark, dangerous side. Interpersonal crime on the Internet is not a new phenomenon, but one that in general has not been widely examined or explored. In fact, many people often minimize the importance and impact of interpersonal violence and crime on the Internet because it is not physical and people sitting in front of their computers are viewed as being safe within the walls of their home. Interpersonal violence and crime on the Internet, however, can and often does lead to physical world violence and crime. Even if it doesn't ever reach the physical world, interpersonal violence and crime on the Internet can lead to data, property, and financial losses; social, professional, and organizational harm; and severe mental and emotional distress.

Throughout this book, an effort will be made to give readers an understanding of the Internet and the potential dangers therein. The Internet as an evolving technology will be discussed, illustrating how quickly technology advances, offering a wealth of opportunities to those with both pioneering and malicious intentions. Readers will also learn that violence is not a static concept but rather a virus that mutates to overcome countermeasures and how the prevalence of violence can be either inhibited or promoted based on the roles that people take while inhabiting the online world.

This book will introduce a new approach to assessing violence and crime on the Internet, combining the technologies of criminal profiling, threat assessment, and risk assessments. This new approach known as the Behavioral Risk Analysis of Violence Online (B.R.A.V.O.) is a behaviorally driven approach that can assess known and unknown perpetrators across both physical and virtual landscapes, providing authorities with violence and crime risk levels, disruption levels, recommended target action, and investigative direction.

Another extremely important aspect of this book is the classification of crime and violence on the Internet into types and strains, allowing people to understand the motivation and behaviors of online perpetrators. Readers will be exposed to the signs and symptoms of violence and crime on the Internet

to help them become better at detecting and interpreting behavior they observe online. This section of the book will also familiarize readers with general violence prevention and intervention principles, as well as safety and survival strategies.

The second part of this book will familiarize readers with the different mediums and interfaces involved with the Internet and exemplify how those with violent or criminal intentions can exploit these mediums. In great detail, readers will be exposed to the major strains of Internet violence and crime and will be given real-world examples of how violence and crime truly work on the Internet, hopefully expanding their detection and awareness abilities.

The final section of the book will highlight some of the difficulties faced by organizations, schools, colleges, businesses, law enforcement, and lawmakers in combating Internet violence and crime. In this section of the book, readers will obtain comprehensive steps for staying safe on the Internet.

Overall, the purpose of this book is to identify all of the different types of interpersonal violence and crime that a person may encounter on the Internet while exploring cyberspace, so that they can then be examined and placed in the context of how violence and crime manifest themselves in the physical world. Comparing interpersonal violence and crime on the Internet with interpersonal violence and crime in the physical world will help inform ways to effectively prevent and respond to the dangers that are present on the dark side of the Internet. Ultimately then, after reading this book a person will not only know how to recognize and detect interpersonal violence and crime on the Internet but also be able to effectively avoid the snare of the Net by being safer, smarter, and more informed "Netizens" of cyberspace–Netizens who are capable of taking the necessary steps to insulate and defend themselves from would-be cyberpredators.

E.M.A.

ACKNOWLEDGMENTS

I have been incredibly fortunate over the years in that I have been surrounded by an incredible group of people both professionally and personally. It is thanks to many of these people that this project was competed. First and foremost I want to thank my wife Michelle for her love, support, and patience with me, as well as her constant encouragement in the writing of this book.

I would like to give special thanks and gratitude to Eoghan Casey, Lavita Nadkarni, and John Nicoletti for all their assistance and for helping this project reach its completion. The three of you allowed this project to be born and helped guide it in its earliest phase. Your time and feedback also laid the groundwork for what this book was to become.

Professionally, it is also important to mention Nicoletti-Flater Associates and give thanks to John Nicoletti and Lottie Flater for providing an environment where staff can find support and guidance and are encouraged to succeed. I would also like to acknowledge and thank Sally Spencer-Thomas for her time and advice on writing a book, and Cristin McCaskill for providing her time and feedback in reviewing this work.

I have also received an incredible amount of support personally on this project. In particular, I would like to thank my parents, David and Carrie, and my grandfather, Lee, for their love and support. The three of you have always been there for me and believed in my ability to accomplish whatever I set out to do. For this, I give my love and thanks.

Finally, I would like to thank my friends Matt and Mark, as well as the rest of my family, friends, and coworkers, who are too many to name. I thank you all for your ongoing friendship and support over the years. A special thanks goes to Zach for his role in this project, since he was the one who nudged me into the Internet in the first place.

CONTENTS

VIOLENCE GOES TO THE INTERNET

Part 1

UNDERSTANDING AND ASSESSING VIOLENCE ON THE INTERNET

Chapter 1

ENTER THE INTERNET

The Internet exists in contradiction. It is a world and universe of its own, existing basically without substance or boundary, within a world that is governed by physical laws, quantifiable physical space, and limited resources. The world within which the Internet exists is also a world that is founded on the idea of control. The Earth and her resources need to be controlled, land and geography need to be controlled, nation-states fight to control themselves and often attempt to control others, states are controlled, populations are controlled, people are controlled, and some would argue that even thoughts are controlled.

Enter the Internet. Many people believe the Internet is the last place where privacy, freedom, and anarchy still exist. Practically speaking, there are no laws on the Internet, for it has no governing body, no corporation that owns its rights, and no board of directors making decisions about the Internet's future based on profit shares and net sales. People from all over the world make up the Internet and drive its content, direction, and focus. Part of what some argue makes the Internet so great is that it is an open and nonjudgmental environment. The Internet accepts any ideas, any thoughts, and any interests. Anything goes on the Internet and often does. The Internet has created a true melting pot where all sorts of people come together as a community. In many ways the Internet, in its virtual splendor, has created community and solidarity where once there was isolation and solitude. Many individuals and groups that once avoided interpersonal connection due to the risks that it might involve are now free to form virtual bonds with others while preserving their sense of isolation, anonymity, and, most importantly, safety.

As is true in any community, the Internet has a light, safe side, and a dark, dangerous side. To date, a great deal of attention has been given to understanding certain aspects of the dark side of the Internet. Specifically, people have strived to understand hacking, computer security, and corporate and

industrial crime. Some examples of such works include *Incident Response: Investigating Computer Crime* (Prosise & Mandia, 2001), *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (Skoudis, 2001), *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community* (The Honeynet Project, 2001), *Cybercrime: Security and Surveillance in the Information Age* (Douglas, Loader, & Loader, 2000), *Fighting Computer Crime: A New Framework for Protecting Information* (Parker, 1998), *Internet Besieged* (Denning, 1998), and *Crime, Deviance, and the Computer* (Hollinger, 1997). There are also a number of websites that deal with corporate and industrial crime on the Internet.

Far less attention, however, has been paid to the less tangible aspects of the dark side of the Internet that can ensnare the individual person. Interpersonal crime on the Internet is not a new phenomenon, but one that in general has not been widely examined or explored. In fact, many people often minimize the importance and impact of interpersonal violence and crime on the Internet because it is not physical and people sitting in front of their computers are viewed as being safe within the walls of their home. Further, many people feel that interpersonal violence and crime on the Internet is an avoidable problem if people would simply turn off their computers. Interpersonal violence and crime on the Internet, however, can and often do lead to physical-world violence and crime. Even if it never reaches the physical world, interpersonal violence and crime on the Internet can lead to data, property, and financial losses; social, professional, and organizational harm; and severe mental and emotional distress.

There are certain types of interpersonal crimes, such as cyberstalking, identity theft, and child pornography, that have been studied in some detail; other types of interpersonal Internet crime, such as those perpetrated by religious cults and hate groups, have received less-thorough attention. There are still other forms of Internet crime and violence, such as cyberterrorism and cyberwarfare, that have only entered the public's awareness since the start of the current millennium. This trend and focus are also reflected in current computer crime legislation. For example, there has been fairly strong legislation both passed and proposed concerning cyberstalking, child pornography, and fraud; laws pertaining to other types of interpersonal crime on the Internet are basically nonexistent or severely lacking.

The purpose of this book is to identify all the different types of interpersonal violence and crime that a person might encounter on the Internet while exploring cyberspace, so that they can then be examined and placed in the context of how violence and crime manifest themselves in the physical world. Comparing interpersonal violence and crime on the Internet with interpersonal violence and crime in the physical world will help inform ways to effectively prevent and respond to the dangers that are present on the dark