THE CYBER PREDATORS

Ever wondered who lurks in the shadows of the Internet's vast landscape, balancing opportunity and risk? *The Cyber Predators* takes you on a revealing journey into the enigmatic world of Dark Triad/Tetrad personalities: psychopaths, Machiavellians, narcissists, and sadists, tackling the urgent issue of online crime as a global crisis. Drawing from cutting-edge research, this book synthesizes knowledge, exploring the motives and tactics that distinguish Dark Triad/Tetrad individuals. Offering unique expertise, it serves as an essential reference for scholars, practitioners, and the public, distinguishing itself with its consolidated and up-to-date approach. Navigating through diverse digital realms – from social media addiction to cyberbullying, hacking, and workplace deviance – this book unravels the complex interplay between Dark Triad/Tetrad personalities and cyber misconduct. Ideal for postgraduate students, it provides interdisciplinary insight, drawing from various scientific fields, making it a valuable resource for understanding cybercrime and its perpetrators.

AARON COHEN is Professor of Management at the University of Haifa. He has published about 100 papers in peer-reviewed journals. Noteworthy among his works are *Multiple Commitments in the Workplace: An Integrative Approach* (Taylor & Francis, 2003) and *Counterproductive Work Behaviors: Understanding the Dark Side of Personalities in Organizational Life* (Routledge, 2018).

THE CYBER PREDATORS

Dark Personality and Online Misconduct and Crime

AARON COHEN
University of Haifa

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781009416863

DOI: 10.1017/9781009416849

When citing this work, please include a reference to the DOI 10.1017/9781009416849

First published 2024

A catalogue record for this publication is available from the British Library

A Cataloging-in-Publication data record for this book is available from the Library of Congress

ISBN 978-1-009-41686-3 Hardback
ISBN 978-1-009-41685-6 Paperback

To Ruti Zohar for her endless support and encouragement and to Vana (and Mesi for a short time) for just being there for me.

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-41686-3 — The Cyber Predators
Aaron Cohen
Frontmatter
More Information

Contents

Tables

Preface

Millions worldwide watched *The Tinder Swindler*, a British actual crime documentary film released on Netflix in February 2022. The film presents a true Israeli man, born Shimon Hayut, who traveled around Europe, presenting himself as the son of Russian-Israeli diamond tycoon Lev Leviev, alias the Diamond King. He used Tinder's dating application to contact women, presenting himself as Simon Leviev and tricking them into lending him the money he would never repay (Zhou, 2023). The frauds he was behind, allegedly, were very similar. He would charm women with generous gifts and take them to dinners on private jets using money he borrowed from other women he had previously conned. He would later pretend he was being targeted by his "enemies," often sending the same messages and images to each woman, indicating that he had just been attacked with a knife but that his bodyguard had saved him and was hurt. He then asked his victims to help him financially due to the breach of "security," supposedly hindering his use of his credit cards and bank accounts; the women often took out bank loans and new credit cards to help. He would then use the money gained through the deception to lure new victims while essentially operating a Ponzi scheme. Later, he would pretend to repay his victims by sending forged documents showing fake bank transfers and then breaking off contact with the victims. Sometimes, he would even go as far as to threaten them and use manipulation to get more money from his victims. It is estimated that he swindled $10 million from people across the globe (The Tinder Swindler, 2022; Osborne, 2022).

The Web has a crucial role in Shimon Hayut's cons. First, he used Tinder to introduce himself as Simon Leviev and to "hunt" his prey. Then, many parts of the "love bombing" stage occurred on Web applications. Then, after the "love bombing" stage, he used WhatsApp and other Web applications to show his victim a fake scene in which he or his bodyguard were in danger. Finally, the money he asked for was mostly transferred via the Internet.

Many who watched this film have shaken their head, wondering how women could be allegedly hoodwinked out of millions of dollars. To understand this, one must realize Shimon Hayut's personality and those of his victims. According to Campbell (2022), people with dark personality traits such as narcissism and psychopathy are likelier to perpetrate romance scams. These individuals lack empathy, lie for self-gain, and manipulate others. Narcissists are incredibly charming in the initial phases of a relationship, which hooks the target, but once the hook is in, control and exploitation ensue. According to Johnston (2022) and Christensen (2022), Hayut behaved like a psychopath. His pattern of deceit, manipulativeness, apparent indifference to the consequences of his actions, superficial charm, lack of empathy, and lack of remorse are all behaviors that certainly head us in that direction. According to Hillier and Greig (2022), Hayut's personality is shaped by the darker side of personality traits, namely, the Dark Triad traits (narcissism, psychopathy, and Machiavellianism) or Dark Tetrad (with the addition of sadism).

As for the victims, Campbell (2022) explained that for various reasons, some people are not successful in relationships, which puts them at risk of being scammed. The history of difficulty may stem from childhood (e.g., bad parenting) or low-quality adult relationships, but either way, these individuals are vulnerable to victimization. When a "partner" requests favors or breaks promises, those with a negative relationship history are inclined to remain committed and indulge the swindler rather than breaking it off. A more general explanation was advanced by Bohns (2022), who contended that Hayut's manipulations relied on the nature of most people to trust others over distrusting them, believing them over doubting them and going along with someone's self-presentation rather than embarrassing them by calling them out. The tendency to trust, believe, and go along with other people's explanations of events may seem disadvantageous.

Furthermore, these inclinations can indeed expose people. Nevertheless, without trust, there is no cooperation; without assuming others are telling the truth, there is no communication; and without accepting people for what they present to the world, there is no foundation for building a relationship. In other words, the very features that look like glitches when exploited are the essence of what it means to be human (Bohns, 2022). The fundamental nature of most people to trust others is the core ammunition of dark personalities, specifically the Dark Tetrad.

The Dark Triad/Tetrad and Cyber Deviance

Shimon Hayut is only one example. Many, like him, males and females, perform many unethical, misconduct, and criminal activities across numerous aspects of life. Romance frauds are only one example of one aspect. This book is about them and their misconduct and criminal activities in social media networks, the most popular platforms our days. The Dark Tetrad traits present four related personalities but are also independent.

Narcissism is described as someone needing admiration and who lacks empathy for others. Other aspects are feelings of grandiosity, self-centeredness, and a sense of entitlement, through which they take advantage of others (VandenBos, 2007, APA Psychology Dictionary). Psychopathic personalities had been a synonym for antisocial personality disorder […] "the presence of a chronic and pervasive disposition to disregard and violate the rights of others. Manifestations include repeated violations of the law, exploitation of others, deceitfulness, impulsivity, aggressiveness, reckless disregard for the safety of self and others, and irresponsibility, accompanied by lack of guilt, remorse, and empathy" (VandenBos, 2007, APA Psychology Dictionary, p. 65). Machiavellianism is defined as a personality trait marked by a calculating attitude toward human relationships and a belief that ends justify means, however ruthless. Machiavellians view other people more or less as objects to be manipulated to pursue their goals, if necessary, through deliberate deception (VandenBos, 2007, APA Psychology Dictionary).

A sadistic personality disorder is characterized by cruelty, aggression, and demeaning behavior (Chabrol et al., 2009). Sadism was defined as "cognitions and behaviors associated with the derivation of pleasure from inflicting physical or emotional pain on another person" (Porter & Woodworth, 2006, p. 486). This diagnosis appeared in the Diagnostic and Statistical Manual (DSM)-III-R (American Psychiatric Association, 1987) but was removed and no longer appeared in the DSM (Smith, 2021). However, some scholars consider this removal a mistake (Millon, 2011). In recent years, the interest in sadism has grown mainly because researchers sought that sadism should be added to the Dark Triad traits as an additional personality disorder despite its removal from the DSM (Johnson, Plouffe & Saklofske, 2019). A difference should be made between sadism and everyday sadism (Greitemeyer, 2015). Sadism can be characterized as deriving pleasure from being responsible for others' experiences of pain (Olckers & Hattingh, 2022; Liu et al., 2023). Everyday sadism is a nonclinical form of sadism. Everyday sadism can be conceptualized as a nonclinical form of sadism, differing from clinical sadism in that the individual does not harm others out of the need for cruelty but rather for the pleasure derived from the act (Greitemeyer, 2015; Porter et al., 2014; Perez del Valle & Hand, 2022; Lauder & March, 2023). Recent research has confirmed that everyday sadists find more pleasure in harming other people than nonsadists (Greitemeyer, 2015; Nocera et al., 2022). While the book will use the term sadist in all the following chapters, it should be noted that it relates to everyday sadists.

Online communication has become essential in modern society (Nocera et al., 2022), with 9 in 10 United States adults using the Internet (Pew Research Center, 2019). Most of the world now depends on computers, the Internet, and cellular technology. Individuals now own laptops connected via Wi-Fi, smartphones, and one or more video game systems that may be networked. Cell phones have become a preferred method of communication for most people, especially text messages. In addition, people have multiple email accounts and social networking profiles on various platforms for personal and business use (Holt, Bossler & Seigfried-Spellar, 2022). Social networking sites are an essential part of individuals' lives. People use social networking sites to maintain relationships, create new connections, and engage with events, people, and organizations.

Online social networking has no generalized definition, but it is defined by Boyd and Ellison (2007) as a web service that allows an individual to do three things: (a) generate a public or semipublic profile in a specific system, (b) create a list of users to interact with and browse through the list of contacts, and (c) see what was done by others within the system. There are many benefits of using social networking sites. They (a) elevate the ease in which individuals may form and create online communities, (b) improve collaboration and sharing of information, (c) can lead to the creation of new job roles, (d) allow users to be constantly connected to friends, (e) allow for ease of communication, information transfer, and (f) help break down social boundaries (Hussain, Wegmann & Griffiths, 2021). People are fond of online social networking for entertainment, social contacts, fun, fame, advertisement, and business. However, some people use social networking sites for evil purposes.

Over the past 20 years, digital communication has become increasingly important in the workplace and in individuals' lives. Social media has become popular with younger people as more diverse platforms have become available (Holt et al., 2022; Hand & Scott, 2022). In this era of technology, the popularity of online social networks is increasing among technologically strong and nontechnical people. The availability of the Internet is one of the primary reasons behind the high utilization of online social networking (Boyd & Ellison, 2007). Social networking sites, in particular, provide users with unique platforms to share their information through personalized web pages and interact with others using the Internet. These characteristics enable many people to use social networking sites to satisfy their self-expression needs. On the one hand, "weak tie" network platforms, that is, less reciprocal platforms that lack close emotional support, such as Twitter, satisfy the need of people to get the attention of many users while averting direct communication. On the other hand, the asynchrony of the Internet allows individuals to elaborate their information (Kong et al., 2021).

Compared to the past, making use of cyberspace and communication has increased. It has been expanded in the last decade due to the increasing growth of virtual social networks and free membership, as well as the facilitation of intelligent communication devices such as the increased number of advanced mobile phones leading to a gradual surge in the number of their users. The statistical information regarding this phenomenon is astonishing. Research suggests that 24% of teenagers use social networking sites constantly, and 71% use more than one social networking site. Recent statistics indicate that one-third of the individuals in the world and two-thirds of all Internet users are active social media users (Nikbin, Taghizadeh & Rahman, 2022). As of early 2017, about 2.8 billion people were members of at least one of these virtual social networks, while in 2010, only 0.97 billion of the world's population were members of one of these networks. It is also estimated that by 2020, the number of users of these social networks will increase to 2.95 billion (Soleimani Rad & Abolghasemi, 2021).

In current society, the Internet plays a fundamental role in interpersonal relationships. The Internet became a social environment that could boost positive self-views and had the exceptional ability to integrate into people's lives. There are now 4.57 billion Internet users worldwide, comprising 58.7% of the world's population (Holt et al., 2022). The Internet has changed human connection in profound ways, facilitating a range of diverse and new social relationships and interactions. (Hand & Scott, 2022). Many people around the world utilize social media as a means to connect and engage with others in different ways. For instance, 69% of American adults use Facebook, though there has been a substantial increase in the use of Instagram and LinkedIn to communicate. By contrast, WhatsApp is much more prevalent globally and is the number one messaging application across much of South America, Western Europe, Africa, and some parts of Asia (Holt et al., 2022).

Facebook is the largest social media site, with 2.85 billion active monthly users, while Twitter is also popular, with 340 million users. On Twitter, users can broadcast "tweets" of up to 280 characters, and other users can like, comment on, or "retweet" (share) them. Two ways in which Twitter differs from some other popular social media sites are the extent to which it is utilized heavily by celebrities as well as lay users and the fact that Twitter users who communicate do *not* know each other offline, in contrast to the majority of Facebook users/"friends" (Hand & Scott, 2022). The invention of the Internet and the advancement of its technologies have changed the world and human communication in profound ways.

Today, various online services and ever-evolving social networking sites are ubiquitous in the Western world and keep gaining popularity worldwide in most European countries. North America's Internet penetration is as high as 90% of the population (Bogolyubova et al., 2018). Over a billion people access social networking services daily to broadcast their personal lives, socialize with fellow users, or procrastinate. The heightened importance of social networking sites for social and political discourse has motivated users to join public discussions by expressing their viewpoints on different issues. The above-mentioned information emphasizes the massive use of social networking sites around the globe. While these instances can be seen as advantages, some experiences can make using mobile phones and the Internet more devastating than enjoying their spontaneity (Grigg, 2010). Unfortunately, this development has paved the way for new forms of virtual abuse, often leading to severe real-life consequences for their victims (Koban et al., 2018).

In addition to the stimulating advantages and benefits of social networking sites, there is a negative side to these profound developments. Information systems have "flattened" the world and facilitated communication and trade in ways that would have been impossible without them (Harrison et al., 2018); however, maladaptive innovations using new technologies have followed on the heels of legitimate transactions. The evolution of human behavior due to technological innovations has created unparalleled opportunities for crime and misuse. Over the last three decades, there has been a substantive increase in the use of technology by street criminals and novel applications to create new forms of crime that did not exist. The World Wide Web and the Internet also provide a venue for individuals who engage in crime and deviance to communicate and share information, which is impossible in the real world. As a result, we must begin to understand how and why these changes are occurring (Holt et al., 2022). What makes this new revolution of technology so appealing to misbehavior and crime?

Papapicco and Quatera (2019) provide a compelling logic to the previous question. Following the great Digital Revolution, the "fluid" woman/man changes the perception of what s/he lives and the essence of the experience, which is the "Who is," hence her/his identity: a re-written identity using the computer. Redefining your identity in a digital context is, in many ways, beneficial because it allows you to take time to rethink and choose descriptions, photos, or videos best suited to the desire to be constantly visible. In particular, the strong wave of social networks has initially differentiated the virtual and digital identity constructs. Virtual identity is the set of potentials, expectations, and imaginations that have not yet materialized online.

On the contrary, digital identity results from "rethinking in an online context." Subsequently, the distinction mentioned earlier was canceled with the predominance of the digital identity over the virtual one. It is multiple digital identities because it can be confirmed or disconfirmed, real but also fake, where the subjects can choose different ways to express themselves and interact with other subjects. Indeed, it is above all thanks to the endless possibilities of freedom offered by the Net and to this constant man–machine relationship, which gives rise to a new fragmented "Who," incapable also of distinguishing reality from virtuality, driven by the uncontrollable fantasy of being able to become another from themselves (Papapicco & Quatera, 2019).

Undoubtedly, if, on the one hand, the Net multiplies the possibilities of creating digital identities, on the other, lacking distinctive indices to depict, such as the tone of the voice or particular facial expressions, traits, that is, that belongs only to the person as dematerialized (a physical Chi), virtual spaces provide more freedom to avoid being identified. On the one hand, digital identity is in extreme need of anonymity because it allows open discussion of very intimate topics in relative security; on the other hand, however, the mere omission of the name could give rise to hostile behavior; it can be to encourage aggression because it makes the behavior more uninhibited, less conditioned by conventions and social norms. Anonymity is characterized by the desire not only to authenticate but also to act in an invisible and sometimes provocative manner: This is one of the darkest sides of the Web (Papapicco & Quatera, 2019).

The spread of the Internet has fundamentally changed the forms of interaction that people enter with each other and has created new opportunities for building their identity and self-esteem. On the one hand, by hiding their physical appearance, people can express themselves more freely and openly. By contrast, on the other, they can hide or fabricate their data, such as gender, education level, financial situation, and many others. This way, Internet users can express their "other self," often fundamentally different from the one that dominates in real life. This also applies to pathological personality traits that can be projected into cyberspace and treated as a specific social environment. Its structural and functional properties favor this, such as anonymity, the lack of nonverbal interaction indicators, asynchrony of interaction, and the lack of clearly defined standards. Unfortunately, these properties are also used to commit punishable offenses (Kong et al., 2021).

Another reason that makes cybercrime so attractive is the ubiquity of this technology that makes it easy for individuals to gain access to the tools necessary to offend with relative ease. The prices of computers have dropped substantially over the last decade, making it very easy to acquire such equipment. In addition, smaller portable computers, such as the iPad and smartphones, which can connect to the Internet through cellular technology, have also become common. As a result, offenders can readily acquire and access information from anywhere through these resources. If people cannot afford to buy these devices independently, they can always use computers in Internet cafes and public libraries for free or at a small cost. Thus, there are minimal barriers to computer technology globally. Also, technology acts as a force multiplier in that computer and computer-mediated technology allow a single person to engage in crimes that otherwise would involve multiple people and complex schemes to target such a significant number of victims. In online environments, offenders can target thousands of victims at a time worldwide within seconds (Holt et al., 2022).

Although these online connections are associated with positive social benefits, enabling quick and easy social interaction, the Internet also promotes a sense of anonymity and decreased accountability, self-awareness, and inhibition, which can encourage deindividuation. Online deindividuation may foster the manifestation of negative, online antisocial behavior, including cyberbullying, trolling, cyberstalking, and online aggression, collectively called cyber abuse (March et al., 2022). Further, some online antisocial behaviors may be illegal, criminal activity, such as cyber fraud and child pornography use, and thus approximate the definition of cybercrime. The online antisocial behaviors that characterize cyber abuse and cybercrime are not specific to a single culture and are considered a global issue (March, 2022). Online social networking has also become a significant platform for cybercriminals to perform several types of crimes. A considerable amount of data on social media is being utilized for several criminal purposes. The attacks' rate, types, and complexity are increasing drastically due to such big platforms where people are available relentlessly (Boyd & Ellison, 2007). Some harmful acts identified within these communication media are bullying, harassment, assault, abuse, and stalking. In the United Kingdom, for instance, cyberbullying has been used as a common phrase for most of these subsets of aggressive acts (Grigg, 2010).

Computers and computer networks (i.e., an interconnected collection of autonomous computers that allow an easy exchange of information between users) have become an integral part of American industry, business, and government. Consequently, their efficient operation is increasingly critical to the survival of the United States and its organizations. Unfortunately, however, next to supporting legitimate business activities and facilitating opportunities to interact with employees, clients, and vendors, the heavy reliance of large organizations on computers and computer networks increases their vulnerability to a wide range of cyber-dependent crimes (i.e., all these crimes that emerge as a direct result of computer technology and the Internet and that could not exist without it). Indeed, numerous reports suggest that large corporations and governmental agencies experience a wide range of computer-focused crimes, including system-trespassing (or hacking), website defacement, Distributed Denial of Service attacks, and malicious software infections, with an estimated $400 billion annual cost to the global economy from these crimes (Maimon et al., 2017).

Cybercrime is now a growing threat because, as aforementioned, the number of people using the Internet is increasing worldwide, and digital technology tools do not require specialist knowledge. Cybercrimes are committed not only by individuals but also by organized criminal groups. Particular attention should be paid to individuals exhibiting psychopathic personality traits, which pose an exceptionally high threat to Internet users. This risk is greater if the group of axial symptoms of psychopathy is accompanied by high intelligence. That is why Internet users who meet these criteria more often commit various cybercrimes, and their offenses are more harmful to victims. It should be remembered that victims of antisocial behavior online experience at least similar effects, both material and mental, as victims of criminals operating in real life. Some authors even claim that cybercrime leads to more severe and longer-lasting consequences, especially for the mental health of victims, for example, depression, chronic anxiety, and low self-esteem (Nicol, 2012; Jung et al., 2014). This group of people, also known as the Dark Triad traits, has the high potential to use the Web primarily for malevolence. Their behavior on social networking sites will be the focus of this book.

Research has focused on predictors of this behavior to understand how to respond to and manage online antisocial behavior. The Dark Tetrad has emerged as a subclinical trait strongly related to cyber abuse and cybercrime. A systematic review synthesizing the research on the Dark Tetrad personality traits (i.e., Machiavellianism, psychopathy, narcissism, and sadism) concluded that all the traits are with a range of antisocial online behavior (March, 2022; Olckers & Hattingh, 2022). There is a reason why Dark Tetrad personalities are attracted to social networking sites. Cyberspace creates conditions for creating a specific social environment in which the lack of face-to-face contact favors the appearance of the "disinhibition effect," as mentioned earlier. In such conditions, personality traits responsible for antisocial behavior can be enhanced in diversity and frequency. In addition, the basic features of cyberspace can have the effect of "psychological distancing" in some people, the essence of which is to perceive other Internet users as unreal, abstract beings (Perenc, 2022).

"The environment of computers, the Cloud, and the Internet make cyber fraudsters even more elusive than before. This behavior differs from what investigators are used to, and it is something they will have to adapt their methods to. Nevertheless, even cyber-crimes are still likely to be driven by the same psychological profiles found previously; only the behavior may have changed" (the Survey of Corporate responsibility reporting 2013, p. 17, as mentioned in Harrison, Summers & Mennecke, 2018). Of recent interest for social and personality psychologists and law enforcement defenses is the relationship between the Dark Tetrad and subversive behaviors that occur online via social networking sites, their applications, and related websites (Moor & Anderson, 2019).

Perence (2022) elaborates on why psychopaths favor cyberspace and its potential use for purposes that do not follow applicable legal order. These features are also relevant to narcissists as well as Machiavellians and sadists.

1. The anonymity of cyberspace. Psychopath uses this trait to hide or change their identity to avoid responsibility for their actions. In this context, while feeling "invisible" in cyberspace, s/he is convinced of the low probability of being caught and exposed to criminal sanctions. Although some psychopaths may realize that online

activity leaves some traces that may identify them, they think that the amount of these traces is small enough to give them anonymity and a sense of impunity.

2. The lack of nonverbal indicators of interaction between communicating people, such as physical appearance, eye contact, facial expressions, mime, and manner of expression. In such circumstances, interacting partners only need to rely on written words, which can often lead to misunderstandings and conflicts. For example, the mere lack of eye contact in interactions in cyberspace makes it difficult to identify a person committing a particular offense.
3. Asynchrony of interactions. This refers to a certain delay in communication in some online environments that use permanent messages, photo albums, and information that does not require their recipients to react in real time. Asynchrony makes cyberspace users less sensitive to current social norms because there are currently no "guards" who can stop someone's inappropriate behavior online. In addition, the absence of an Internet audience that could monitor the course of interaction means that users do not feel pressured to force them to comply with commonly accepted standards.
4. The lack of clearly defined norms. This promotes the occurrence of reprehensible behavior. Although some social networking sites require compliance with specific laws and policies, most users treat cyberspace as an open area for everyone that can be "conquered" without looking at legal regulations and social norms. Difficulties with implementing universally applicable social norms in cyberspace mean that, at present, one cannot speak of universal Internet culture. One consequence of this is the existence of social networking sites that allow anonymous users to publish all kinds of offensive content, such as calls for the persecution of specific groups of people, the promotion of racist theories, or the unlawful sharing of personal data (Perenc, 2022).

Those mentioned four basic features of cyberspace in practice work in a complementary manner, which promotes the expression of psychopathic features possessed by specific Internet users. In some people, the structural elements of cyberspace may also be conducive to adverse changes in the moral sphere, facilitating their involvement in socially unacceptable behavior. In this respect, they resemble the Dark Tetrads. It primarily relates to the role played by psychological distancing, which limits the influence of moral principles observed daily in direct contact between people. The lack of clearly defined social norms, typical of online contacts, is also essential, contributing to disregarding the potential consequences of offenses committed in cyberspace. This leads to the conclusion that in the case of many people, there is a violation of moral norms in relationships with others in cyberspace, even though these people generally follow these norms in genuine relationships (Perenc, 2022).

However, the intensity of violations in cyberspace is much more vigorous among Dark Tetrad personalities. The above-mentioned features of cyberspace seem to suit them perfectly. They feel highly comfortable performing cyber misbehavior and cybercrime, giving them a tool with a lower likelihood of being exposed and perhaps being accountable and punished. Therefore, the interest in the role of personality traits in determining offenses and deviant behavior in cyberspace has increased in recent years. According to Perenc (2022), there is a clear qualitative difference in personality profiles between cyber deviants and people in the general population who often use digital technology. People classified as cyber deviants generally have higher features, such as a tendency to manipulate and exploit others and no moral inhibitions. Many studies indicate the presence of a solid connection between the Dark Tetrad and cyber harassment, which means that the features of Dark Tetrad personalities occupy a central place in the personality profile of individuals making such offenses (Perenc, 2022).

The media reports increasingly on a variety of crimes performed using cyber. This issue has become a severe problem for society across the globe. Constraining from cyber abuse and crime becomes a vital need in a modern community. To succeed in this mission, there is also a need to understand it better and the personalities behind it, many of them dark personalities. This book responds to this challenge. The goal of this book will be to expose and explore the role of Dark Tetrad personalities in performing cyber misbehavior and crime. The chapters of the book will attempt to cover the issue thoroughly.

Chapter 1, the introduction, will present, define, and explain the two main concepts of the book. Then, it will elaborate on the main characteristics of each Dark Tetrad. Later, it will present the main forms of cyber misbehavior and cybercrime and their adverse outcomes. In its last comments, the chapter will present some main theories explaining why Dark Tetrad personalities are attracted to social media networks as a tool for perming their evil behaviors. Chapter 2 will focus on social media addiction. The chapter will argue that while a certain amount of extra time spent on social media networks can occur for many individuals, an addiction above normal behavior can characterize Dark Tetrad personalities. Finally, the chapter will cover issues of levels of addiction of Dark Tetrad to social network media, theories that explain the causes, and the adverse outcomes of being addicted to social media networking.

Chapter 3 will focus on the potential role of Dark Tetrad personalities on Facebook and other social media platforms. The first section will describe the importance and usage of Facebook in modern life. Then, the chapter will portray the benefits and potential damages included in Facebook. Next, it will present theories explaining Dark Tetrad personalities' attraction to Facebook. The chapter will review the relationship to Facebook for each Dark Tetrad personality. The assumption is that each of the three personalities has its own view and approach regarding the usage of Facebook. The chapter will also cover an important issue discussed in the literature: predicting Dark Tetrad personalities based on Facebook profiles and activities. Chapters 4 and 5 will concentrate on hate behaviors. Chapter 4 will focus on cyberbullying and aggression of Dark Tetrad personalities on social networking sites. Bullying and aggression are severe societal problems, and cyberbullying is no different. Cyberbullying can be viewed as rude/discourteous behaviors through Information and Communication Technologies. The chapter will review the different approaches and definitions of cyberbullying. It will later review the devastating outcomes of cyberbullying. The main parts of the chapter will be to discuss the role and the reasons for Dark Tetrad personalities to be involved in cyberbullying. This will be reviewed separately for each of the dark personalities. The chapter will end with a review of the latest research findings on the relationship between Dark Tetrad personalities and cyberbullying.

Chapter 5 will review Dark Tetrad personalities' involvement in cyber stalking, surveillance, and trolling. Cyberstalking is the stalking of others through electronic access and communication methods, such as using hidden webcams, global positioning system devices, and SpyWare to monitor the victim's behavior and pursuit and contact under anonymity through fake online profiles. First, the chapter discusses the differences between stalking and cyberstalking. The following section will review conceptual explanations for the involvement of Dark Tetrad personalities in cyber stalking and surveillance. The final section will present studies on the relationship between the Dark Tetrad personalities and cyber stalking and cyber surveillance. Cyber trolling and their relationship to Dark Tetrad personalities will be reviewed in the second section of Chapter 6. Trolling is an interpersonal antisocial behavior prominent within Internet culture across the world. Trolling behavior includes starting aggressive arguments

Cambridge University Press & Assessment
978-1-009-41686-3 — The Cyber Predators
Aaron Cohen
Frontmatter
More Information

and posting inflammatory, malicious messages in online comment sections to provoke, disrupt, and upset others deliberately. First, the chapter will review definitions and descriptions of cyber trolling. Then, theories about the reasons behind each Dark Tetrad trait's motives for using trolling behavior will follow. The chapter will later present research findings on the relationship between each of the four dark personalities and trolling.

Chapter 6 will cover one of the most important and devastating issues in cyber misbehavior, namely cybercrime. The chapter will start by describing the different forms of cybercrime, such as hacking, cyberattacks, phishing, insurance fraud, online consumer fraud, and more. The following section will present theories regarding the reasons behind each Dark Tetrad motive to perform cybercrimes. The final section of the chapter will present findings about the relationship between each Dark Tetrad trait and the different forms of cybercrime.

Chapter 7 will present another vital aspect regarding Dark Tetrad involvement in cyberspace: Dark Tetrad and intimate cyber relationships. First, the chapter will review the different forms of cyber abuse in romantic relationships, such as cyber dating, revenge pornography, and ghosting. Next, the chapter will review the specific role of each Dark Tetrad personality in cyber relationship abuse and the motives behind their behavior in this setting. Finally, the chapter will present research findings on this relationship.

Chapter 8 will focus on the work setting. The importance of understanding cyber misbehavior in the workplace and the devastating outcomes of cyber misbehavior will be presented first. After that, a description of the different ways of cyber misconduct in the work setting will be reviewed, such as cyberloafing, cyber aggression, and cyberbullying. Next, theories about Dark Tetrad personalities' motives for workplace cyber misconduct will follow. Finally, the chapter will end with presenting research findings about the relationship between the four dark personalities and cyber misbehavior in the workplace.

The book will end with Chapter 9, presenting the previous chapters' conclusions. The chapter will start with briefly reviewing the main findings presented in the earlier chapters. The conceptual contribution of the book will be explained later. The next section of the chapter will discuss the practical implications of understanding the impacts of Dark Tetrad cyber misbehaviors in the different settings presented in the book. Suggestions for better coping with Dark Tetrad cyber misconduct will follow this. The final section of the chapter will suggest future research agendas on this vital issue.

An important note is that both terms, Dark Triad and Dark Tetrad, will be used throughout the book. This is unavoidable. While the emphasis will be using the term Dark Tetrad most of the time, in empirical studies that examined the Dark Triad, this will be the term that will be used. The term Dark Tetrad cannot be used when an empirical study only examined the three Dark Triad traits: narcissism, Machiavellianism, and psychopathy. This rationale will guide the usage of the terms throughout the entire book.

This book provides a valuable perspective on one of the most important issues in modern society: cyberspace, cyber misbehavior, and cybercrime. Delving into these issues has become more vital now that rapid technological changes in cyberspace have had substantial effects on the current society around the world. In this new world of cyberspace, cybercrime and misbehavior have emerged as fundamental phenomena around the globe. Therefore, it is no surprise that this book relies on conceptual and empirical studies performed in recent years. A better understanding of this stunnable and worrying phenomenon can provide essential guides and tools to cope with the enormous potential damages of cybercrime and misbehavior.