Preface

The constantly changing landscape of Cyber Behavior challenges experts and practitioners to stay apprized of the field’s most up-to-date research. That is why Information Science Reference is pleased to offer this four-volume reference collection that will empower students, researchers, and academicians with a strong understanding of critical issues within Cyber Behavior by providing both broad and detailed perspectives on cutting-edge theories and developments in the field. This collection is designed to act as a single reference source on conceptual, methodological, technical, organizational, and managerial issues, as well as provide insight into emerging trends and future opportunities within the discipline.

*Cyber Behavior: Concepts, Methodologies, Tools, and Applications* is organized into eight distinct sections that provide comprehensive coverage of important topics. The sections are (1) Fundamental Concepts and Theories, (2) Development and Design Methodologies, (3) Tools and Technologies, (4) Utilization and Application, (5) Organizational and Social Implications, (6) Managerial Impact, (7) Critical Issues, and (8) Emerging Trends. The following paragraphs provide a summary of what readers may expect from this invaluable reference tool.

Section 1, “Fundamental Concepts and Theories,” opens this multi-volume reference with a discussion of Cyber Behavior and the risks and benefits associated with socializing in digital environments. The first chapters of this section, *Communication and Collaboration in a Web 2.0 World* by F. Dianne Lux Wigand and *Knowledge Sharing in the Age of Web 2.0* by François Deltour, Loïc Plé, and Caroline Sargis Roussel, explore how the digital Web is redefining social and professional interactions through ubiquitous networking and near constant connection to people and resources. Topics covered in this section include online communities (*Redefining Participation in Online Community* by Gibrán Rivera Gonzalez and Andrew Cox), online identity (*Communities, Communication, and Online Identities* by Mikko Jäkälä and Eleni Berki), cyberbullying (*Social Networking, Cyber Bullying, and the Role of Community Education* by Michelle Sofo and Francesco Sofo), and cybercrime (*Cyber Criminals on the Internet Super Highways* by Edwin Agwu), among others. The section closes with a discussion of cyberterrorism and the threats brought about by society’s persistent online presence, a topic of great concern and significance to the rest of this book.

Section 2, “Development and Design Methodologies,” continues from the first section by exploring the security and structure of online communities and the inherent effect of Web 2.0 on Cyber Behavior. The section begins with a discussion of risk management and protection against cyberterrorism and cybercrime. Notable chapters include *Cyber Risks in Energy Grid ICT Infrastructures* by Giovanna Dondossola, Fabrizio Garrone, and Judit Szanto; *An Alternative Framework for Research on Situational Awareness in Computer Network Defense* by Eric McMillan and Michael Tyworth; and *Safeguarding Australia from Cyber-Terrorism* by Christopher Beggs and Matthew Warren. Additionally, this section includes chapters dealing with constructive subjects, such as *Designing and Implementing Online Collaboration Tools in West Africa* by Caitlin M. Bentley, *A Framework for Government 2.0 Development...*
and Implementation by Yu-Che Chen, and Virtual Communities of Practice as a Support for Knowledge Sharing in Social Networks by Yóris Linhares de Souza, Fernanda Farinelli, George Leal Jamil, Maria Celeste Reis Lobo de Vasconcelos, and Gutenberg Marques Dias, all of which help to illustrate how Web 2.0 technologies can be implemented to improve the effectiveness of organizations and quality of living for society as a whole.

Section 3, “Tools and Technologies,” investigates the technological facet of Cyber Behavior, including all of the tools and devices that make online interaction possible. The section begins with several chapters that discuss using Web 2.0 as a means to conduct business and interact professionally with others in virtual environments. In Web 2.0 Open Remote and Virtual Laboratories in Engineering Education, Christophe Salzmann, Denis Gillet, Francisco Esquembre, Héctor Vargas, José Sánchez, and Sebastián Dormido show how a virtual learning space can be utilized in even the most tactile of educational disciplines, and An E-Portfolio to Support E-Learning 2.0 by Hedia Mhiri Sellami describes an excellent method of student interaction and sharing of individual work and accomplishments. Online communities are not only for education, however, and can be used for a variety of social and professional interactions, as shown in the chapters Web 2.0 Technologies and Authentic Public Participation by Colleen Casey and Jianling Li and The Meeting Point of Second Life® and Web 2.0 by Ya-Chun Shih. The end of this section returns to the topic of cyber security with the chapter Botnets and Cyber Security by Ahmed Mansour Manasrah, Omar Amer Abouabdalla, Moein Mayeh, and Nur Nadiyah Suppiah and a transition into the next section’s focus on specific applications of the tools mentioned above.

Section 4, “Utilization and Application,” proceeds from the first three sections to describe the particular ways in which Cyber Behavior affects modern life and society. In the working world, organizations are constantly seeking to gain advantage, whether in governmental, business, or military settings. Chapters such as Cyber Command and Control by Michael E. Ruiz and Richard Redmond, Security and Privacy Issues in E-Government by Ramaraj Palanisamy and Bhasker Mukerji, and E-Marketing on Online Social Networks and Ethical Issues by Gajendra Sharma and Li Baoku explore just a few of the potential applications of online interaction and virtual environments. Later chapters in this section focus on social media and online gaming applications, with notable chapters including Norms, Practices, and Rules of Virtual Community of Online Gamers by Shafiz Affendi Mohd Yusof and Using Web 2.0 Features on Social Networks for Word-of-Mouth Effects by Tan Chee Liang, Chua Kok Seng, and Kaung Pye Soe. Finally, the section ends with a focus on e-learning and Web-based learning applications, such as Digital Storytelling with Web 2.0 Tools for Collaborative Learning, by Najat Smeda, Eva Dakich, and Nalin Sharda.

Section 5, “Organizational and Social Implications,” discusses one of the primary concerns in the field of Cyber Behavior: how humans view themselves and interact with one another in an online environment. The founding focus of this section is the concept of virtual communities and an individual’s digital identity, topics which are explored at length in chapters such as E-Behaviour Trends and Patterns among Malaysian Pre-Adolescents and Adolescents by Selvi Salome Gnasigamoney and Manjit Singh Sidhu, Identification vs. Self-Verification in Virtual Communities (VC) by Kathy Ning Shen, and Web 2.0, the Individual, and the Organization by Kerry J. Burner. Though online interaction is a prevalent topic in the modern world, human rights is an equally important concern in virtual environments where avatars, not people, interact. Such issues are discussed in the chapters Virtual Hate Communities in the 21st Century by Glenn T. Tsunokai and Allison R. McGrath; Cyber-Bullying, Personality and Coping among Pre-Adolescents by Constantinos M. Kokkinos, Nafsika Antoniadou, Eleni Dalara, Anastasia Koufogazou, and Angeliki Papatzi; and When the Virtual and the Real Clash by Celia Romm Liver-
more. This section leads into the next with a final discussion of virtual communities and how they can be used to manage constituents and engage team member in new and more effective ways.

Section 6, “Managerial Impact,” examines the Cyber Behavior of leaders and teams interacting in virtual environments for mutual gain. The first chapters in this section illustrate how Web 2.0 technologies can be used for professional development and employee training. *The Pedagogical Considerations in the Design of Virtual Worlds for Organization Learning* by C. Candace Chou and Rama Kaye Hart, for example, demonstrates how organizational leaders can use 3D virtual worlds to train their employees. The next chapters focus on business leadership and customer relationship management, notably *Improving CRM 2.0 through Collective Intelligence by Using CBIR Algorithms* by Yuliana Perez-Gallardo, Giner Alor-Hernandez, and Guillermo Cortes-Robles; *Exploiting Technological Potentialities for Collaborative New Product Development* by Pasquale Del Vecchio, Valentina Ndou, and Laura Schina; and *A Framework for Customer Knowledge Management based on Social Semantic Web* by Marcirio Silveira Chaves, Cásia Trojahn, and Cristiane Drebies Pedron. The last chapters in this section cover cybersecurity and how effective management of digital resources is necessary for the protection of critical infrastructure, as is demonstrated in Joey Jansen van Vuuren, Louise Leenen, Jackie Phahlamolahla, and Jannie Zaaiman’s chapter, *An Approach to Governance of CyberSecurity in South Africa.*

Section 7, “Critical Issues,” investigates the topic of Cyber Behavior with respect to the concerns and needs of users in online communities. This section begins with chapters related to the topics of e-government and citizen engagement, including *The Role of Web 2.0 in the Arab Spring* by Robert A. Cropf, Mamoun Bennamou, and Morris Kalliny, and *Are ICT/Web 2.0 Tools Influencing Civic Engagement in Modern Democracies?* by Indu Nair, Bardo Fraunholz, and Chandana Unnithan. Following this, the second major topic of section seven is social networking and its implications for personal and professional interactions. Notable chapters include *The Role of Social Networking Sites for Language Learning in UK Higher Education* by Billy Brick, *An Examination of the Factors Influencing Consumers’ Visit of C2C Websites* by Amira Trabelsi Zoghli and Mourad Touzani, and *Social Networking (ing) on Facebook* by Robert N. Spicer. This section concludes with *Viewing Cybercommunities through the Lens of Modernity* by Victoria Wang, John V. Tucker, and Kevin Haines, an effective transition into the final section’s discussion of recent developments in the field.

Section 8, “Emerging Trends,” presents a detailed discussion of some of the most prominent topics being explored by researchers of Cyber Behavior. This section covers a broad range of topics such as virtual communities, e-government, cybersecurity, and online identity, among others, demonstrating the sheer ubiquity of these technologies in modern society. Particular chapters of note in this section include *Virtual Communities as Subaltern Public Spheres* by Weiyu Zhang; *Citizens Collaboration and Co-Creation in Public Service Delivery* by Panagiotis Kokkinakos, Sotiros Kousouris, Dimitrios Panopoulos, Dimitrios Askounis, Antonis Ramflos, Christos Georgousopoulos, and Erik Wittern; *Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments* by Eric D. Vugrin and Jennifer Turgeon; and *The “Right to be Forgotten” in the Era of Social Media and Cloud Computing* by Maria Giannakaki. This multi-volume reference concludes with *Using Hybrid Attack Graphs to Model and Analyze Attacks against the Critical Information Infrastructure* by Peter J. Hawrylak, Chris Hartney, Mauricio Papa, and John Hale, a chapter describing one of the most important considerations for the use and improvement of virtual worlds: the security and wellbeing of its users.

As a comprehensive collection of research on current findings related to the development of interdisciplinary technologies, *Cyber Behavior: Concepts, Methodologies, Tools, and Applications* provides researchers, administrators, and all audiences with a complete understanding of the latest advances,
applications, and concepts in Cyber Behavior. Although the primary organization of the contents in this multi-volume work is based on its eight sections, offering a progression of coverage on the important concepts, methodologies, technologies, applications, social issues, managerial considerations, critical concerns, and emerging trends, the reader can also identify specific content by utilizing the extensive indexing system found at the end of each volume. Given the vast number of issues concerning usage, successes and failures, policies, strategies, and applications of Cyber Behavior in countries around the world, *Cyber Behavior: Concepts, Methodologies, Tools, and Applications* addresses the demand for a resource that encompasses the most pertinent research on the technologies being employed to globally bolster the knowledge and implementation of Cyber Behavior.