SpringerBriefs in Cybersecurity

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The *SpringerBriefs in Cybersecurity* series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

More information about this series at http://www.springer.com/series/10634

Samer Al-khateeb • Nitin Agarwal

Deviance in Social Media and Social Cyber Forensics

Uncovering Hidden Relations Using Open Source Information (OSINF)

Springer

Samer Al-khateeb
Department of Journalism,
Media & Computing
Creighton University
Omaha, NE, USA

Nitin Agarwal
Information Science Department
University of Arkansas at Little Rock
Little Rock, AR, USA

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-030-13689-5 ISBN 978-3-030-13690-1 (eBook)
https://doi.org/10.1007/978-3-030-13690-1

Library of Congress Control Number: 2019935524

Samer would like to thank his parents, Ihsan Al-khateeb and Basima Al-Qaraghuli, and his siblings, Samar, Saja, and Hasanain Al-khateeb, for all the care and support provided to him throughout his life. He also would like to especially thank his wife Lina Al Azzawi for all the love, patience, and positive vibes given to him at the time of writing this manuscript. Nitin Agarwal would like to dedicate this book to his family and friends with much love and gratitude for everything. Without all their encouragements, this endeavor would not be possible.

Foreword

This book describes the methodologies and tools used to collect, analyze, and visualize social media data and conduct social cyber forensic analysis. By applying these methodologies and tools on various events observed in the case studies contained within, their effectiveness is highlighted. The methodologies blend computational social network analysis and cyber forensic concepts and tools in order to identify and study information competitors. Through cyber forensic analysis, metadata associated with propaganda-riddled websites is extracted. This metadata assists in extracting social network information such as friends and followers; communication network information, i.e., networks depicting flows of information among the actors such as tweets, replies, retweets, mentions, and hyperlinks; and social media footprint, i.e., users' or groups' activity on other social media sites. Through computational social network analysis, the authors identify influential actors and powerful groups coordinating the disinformation campaign. A blended social cyber forensic approach allows them to study cross-media affiliations of the information competitors. For instance, narratives are framed on blogs and YouTube videos, and then Twitter and Reddit, for instance, will be used to disseminate the message. Social cyber forensic methodologies enable researchers to study the role of modern information and communications technologies (ICTs) in the evolution of information campaign and coordination. In addition to the concepts and methodologies pertaining to social cyber forensics, this book also offers a collection of resources for readers including several datasets that were collected during case studies, up-to-date reference and literature surveys in the domain, and a suite of tools that students, researchers, and practitioners alike can utilize. Most importantly, the book demands a dialogue between information science researchers, public affairs officers, and policymakers to prepare our society to deal with the lawless "wild west" of modern social information systems triggering debates and studies on cyber diplomacy.

Springer Nature, Cham, Switzerland
March 2018

Christopher T. Coughlin

Preface

In order to address the problem of deviance in social media, we need to understand the power of social media analytics, the importance of open-source information (i.e., information from publicly available sources), and the impact of combining both to study deviant groups and tactics. We wrote this book to raise awareness of the deviant usage of social media by various groups, both virtual or physical. Hence, we introduce and blend a set of graph-theoretic concepts, social network analysis, and social cyber forensic tools and methodologies.

The readers will understand the aforementioned concepts, analysis, and tools to collect various social media data, and the metadata associated with various entities then analyze the collected data and derive insights. The methodologies and tools that we introduce throughout the book have been tested on many real-world events, e.g., the anti-NATO propaganda campaigns, ISIS/Daesh/ISILs propaganda, and the cyber campaigns of Blackhat hackers on social media. These methodologies have been developed with underpinnings in sociological theories of collective action, cyber forensic science, graph theory, and social network analysis. At the end of this text, we present a set of case studies that bring together all the concepts introduced in this book.

This book is suitable for undergraduate and graduate students as well as analysts who are interested in studying the problem of deviance in social media. After reading this book, readers will be enriched with a knowledge of various off-the-shelf tools. We hope this book can jump-start their skills on collecting, analyzing, and visualizing various social media datasets and use social cyber forensic analysis to unveil hidden relations. The book is written considering the wide range of disciplines that would benefit from it. For this reason, the concepts and tools covered in this book require absolutely zero technical background.

Omaha, NE, USA
Little Rock, AR, USA
December 2018

Samer Al-khateeb
Nitin Agarwal

Acknowledgments

We thank many colleagues who made substantial contributions in various ways to this project. The members at the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS) group at UA-Little Rock made this project much easier and enjoyable. We are grateful for their comments.

We really appreciate Springer and particularly Christopher Coughlin, Editor, for helping us throughout this project.

The research presented in this book is funded in part by the US National Science Foundation (IIS-1636933, IIS-1110868), US Office of Naval Research (N00014-10-1-0091, N00014-14-1-0489, N00014-15-P-1187, N00014-16- 1-2016, N00014-16-1-2412, N00014-17-1-2605, N00014-17-1-2675), US Air Force Research Laboratory, US Army Research Office (W911NF-16-1-0189), US Defense Advanced Research Projects Agency (W31P4Q-17-C-0059), Arkansas Research Alliance, the Jerry L. Maulden-Entergy Fund at the University of Arkansas at Little Rock, and Creighton University's College of Arts and Sciences. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations. The researchers gratefully acknowledge the support.

Last, and certainly not least, we thank our families, for supporting us through this fun but time-consuming project. We dedicate this book to them, with love.

Contents

About the Authors

Samer Al-khateeb is an Assistant Professor in the Department of Journalism, Media and Computing, College of Arts and Sciences, at Creighton University and a former Postdoctorate Research Fellow at the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS) at the University of Arkansas at Little Rock (UA-Little Rock). He obtained his Ph.D. in Computer and Information Sciences, a master's degree in Applied Science, and a bachelor's degree in Computer Science from UA-Little Rock. He studies deviant acts (e.g., deviant cyber flash mobs and cyber propaganda campaigns) on social media that are conducted by deviant groups (e.g., Daesh, Black hat hackers, and Propagandist) which aim to influence individual's behaviors and provoke hysteria among citizens. He also studies the type of actors these deviant groups use to perform their acts, i.e., are they human (e.g., Internet trolls) or automated actors (e.g., social bots) by leveraging social science theories (e.g., the theory of collective action), social network analysis (e.g., centralities and community detection algorithms), and social cyber forensics (e.g., metadata collection to uncover the hidden relations among these actors across platforms). He has many publications including book chapters, journal papers (e.g., *Defence Strategic Communications*; *Journal of Digital Forensics, Security and Law*; *Journal on Baltic Security*; and the *IARIA (International Journal on Advances in Internet Technology))*, conference proceedings, and conference presentations. He won various awards such as the Staff Achievement Award for Educational Achievements, Excellence in Research Award, Outstanding Graduating Student Award (Master's Level), Who's Who Among Students in American Universities and Colleges, the Best Paper Award, 2nd Place Most Innovative Award, and 2nd Place Societal Impact Award, among others.

Nitin Agarwal is the Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor of Information Science at the University of Arkansas at Little Rock. He is the Founding Director of the Collaboratorium for Social Media and Online Behavioral Studies (COSMOS) at UA-Little Rock. His research aims to push the boundaries of our understanding of cyber social behaviors that emerge and evolve constantly in the modern information and communication platforms with

applications in defense and security, health, business and marketing, finance, and education. At COSMOS, he is leading projects funded by over $10 million from an array of federal agencies, including US National Science Foundation, Office of Naval Research, Army Research Office, Air Force Research Laboratory, Defense Advanced Research Projects Agency, and Department of State, and plays a significant role in the long-term partnership between UA-Little Rock and the Department of Homeland Security. He developed publicly available social media mining tools, viz., Blogtrackers, YouTube Tracker, and Focal Structure Analysis used by NATO Strategic Communications and public affairs, among others. Dr. Agarwal participates in the national Tech Innovation Hub launched by the US Department of State to defeat foreign-based propaganda.

His research contributions lie at the intersection of social computing, behavior-cultural modeling, collective action, social cyber forensics, AI, data mining, and machine learning. From Saudi Arabian women's right to drive cyber campaigns to autism awareness campaigns to ISIS and anti-West/anti-NATO disinformation campaigns, at COSMOS, he is directing several projects that have made foundational and applicational contributions to social and computational sciences. He has published 8 books and over 150 articles in top-tier peer-reviewed forums with several best paper awards and nominations. Dr. Agarwal obtained Ph.D. from Arizona State University with outstanding dissertation recognition in 2009. He was recognized as one of "The New Influentials: 20 In Their 20s" by Arkansas Business in 2012. He was recognized with the university-wide Faculty Excellence Award in Research and Creative Endeavors by UALR in 2015. Dr. Agarwal received the Social Media Educator of the Year Award at the 21st International Education and Technology Conference in 2015. In 2017, the *Arkansas Times* featured Dr. Agarwal in their special issue on "Visionary Arkansans: A Celebration of Arkansans with ideas and achievements of transformative power." Dr. Agarwal was nominated as International Academy, Research and Industry Association (IARIA) Fellow in 2017, Arkansas Academy of Computing (AAoC) Fellow in 2018, and Arkansas Research Alliance (ARA) Fellow in 2018.

Visit http://ualr.edu/nxagarwal/ for more details.

Acronyms

API	Application Programming Interface
ASAs	Automated social actors/agents
BRJP	Brilliant jump exercise
CA	Collective Action
CCA	Cyber collective action
CFM	Cyber flash mob
DCFM	Deviant Cyber Flash Mob
DDoS	Distributed denial-of-service
DHN	Deviant hacker networks
EEAS	European External Action Service
FM	Flash mob
FSA	Focal Structures Analysis
ICSR	International Centre for the Study of Radicalization and Political Violence
ICT	Information and communications technology
I2P	Invisible Internet Project
IRC	Internet Relay Chat
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
ITAR	Information Telegraph Agency of Russia
LIWC	Linguistic Inquiry and Word Count
MMOGs	Massive Multiplayer Online Games
MUDs	Multi-User-Domains
NATO	The North Atlantic Treaty Organization
NIGMS	US National Institute of General Medical Sciences
NodeXL	Network Overview, Discovery and Exploration for Excel
NRNB	National Resource for Network Biology
NSMT	New Social Movement Theory
ODBC	Open Database Connectivity
ODGs	Online Deviant Groups
ORA	Organizational Risk Analyzer

OSINF	Open-Source Information
OSN	Online Social Network
PAO	Public Affairs Officer
SCF	Social cyber forensics
SNA	Social network analysis
TAGS	Twitter Archiving Google Sheet
TASS	Telegraph Agency of the Soviet Union
TCOs	Transnational Crime Organizations
TOR	The Onion Router
TRJE	Trident Juncture Exercise
WCE	Web Content Extractor
WoW	World of Warcraft
WTC	Web Tracker Code

List of Figures