Digital Influence Mercenaries: Profits and Power Through Information Warfare

by

James J.F. Forest

Naval Institute Press (Forthcoming 2021)

Table of Contents

Preface

My first book on influence warfare, published in 2009, examined propaganda, psychological operations and disinformation, especially how websites, blogs, e-mail, online videos, digital magazines and other such things were used to shape beliefs, attitudes and behaviors. The central theme of that book was how governments were competing with terrorists for influence and support in the public domain, and particularly on the Internet. More recently, my research has focused on how nation-states (like Russia, China, Iran and the Philippines) have embraced new forms of online information operations against foreign and domestic audiences, often in pursuit of political goals. But I also found many perpetrators of influence operations that were neither states nor terrorists. Some were merely individuals who had found a way to profit from disseminating disinformation and provoking emotions via social media platforms, while others were teams, or even formal companies with expertise in data analysis and online marketing. In the end, as with many journeys of intellectual exploration, I discovered that what I've been calling influence warfare is far more complicated than I had originally envisioned.

Digital forms of influence warfare encompass much more than state-sponsored meddling in U.S. elections, terrorist movements seeking to inspire and indoctrinate new recruits, or

political parties seeking to provoke and deceive target audiences. There is a massive profit-making enterprise, built to function upon (and take advantage of) an even larger profit-making enterprise created by social media platforms with hundreds of millions of users worldwide. Throughout this enterprise there are clear and recognizable strategies and tactics used to manipulate the perceptions and behaviors of others. The mercenary's arsenal of methods and tactics include deception (including information deception, identity deception, and engagement deception), emotional provocation, and outright attacking the target (to include bullying, hacking, exposing embarrassing information online, etc.). The first several chapters of this book will examine these methods (as well as the underlying economics of this industry), with many examples to illustrate what is meant by the term digital influence mercenaries, what they do and why.

Digital influencing involves people exploiting other people, using the tools and platforms of social media as a means to an end. But these operations are not only about technology—automated fake accounts, data algorithms, deepfake videos, and so forth. As reflected in the chapters of this book, this arena of activity involves the intersections of human behavior, beliefs, preferences, technology, power and profit. The targets of these digital influence operations are you, me, and the billions of other people worldwide who are providing free and unfiltered access to themselves by posting photos, personal revelations, telling people where they are at a given moment, publicly declaring their likes and dislikes, and showcasing who their friends and family are. Further, because of the profit models that pervade the attention economy, Internet firms track a user's patterns of behavior so they can formulate the right kinds of advertising campaigns. Just as every click and keystroke can be monitored, recorded, and used for analysis that generates advertising profits for the Internet companies, the same data inform the strategies and tactics of digital influence.

There are also important psychological dimensions to the effectiveness of digital influence efforts, as we'll explore in Chapters 3 thru 7. For example, successful mercenaries understand that human beings typically have a strong desire to avoid uncertainty. We adopt a wide range of decisions and behaviors that are meant to reduce uncertainty and mitigate its effects. Unfortunately, these decisions and behaviors create opportunities that digital influence mercenaries can exploit for their own purposes. For example, we know that exploiting uncertainty and fear is a powerful way to grab attention and to provoke emotional or behavioral responses among the targets of an influence effort. There are also ways to manufacture uncertainty where there once was none—such as spreading false information about scientific evidence linking smoking and health risks.

At the same time, when we have strong beliefs or confidence about the world around us (and our place within it), we tend to prefer only information that bolsters our confidence, while avoiding or rejecting information that contradicts what we believe. We like to see things that support our beliefs, as this makes us feel good about choices we have made. But this also creates opportunities that digital influence mercenaries can exploit for their own purposes. For example,

influence operations can use provocation tactics to challenge our beliefs, compelling us to defend our beliefs in something we feel strongly about.

Provoking a reaction is a cornerstone of digital influence operations, because it generates online engagement (e.g., getting us to click on a link, post some sort of comment, reply to a message that offends us, etc.), and that engagement can generate revenue for the mercenary. They may be paid to do such things, but they can also focus their efforts on luring people to an ad-heavy website, where visitors will see loads of bias confirming information, while the mercenary watches their ad revenues increase. Further, mercenaries are increasingly able to exploit media outlets, some of whom will repeat false narratives while others attempt to counter those with fact-checking and condemnation—in both cases, amplifying the original disinformation.

Confronting the efforts of digital influence mercenaries will require a whole-of-society effort, as we'll discuss briefly in the concluding chapter. Social media platforms have already begun tagging disinformation with warning labels, while coordinated inauthentic behavior is being identified and blocked. Websites, Facebook pages, and YouTube channels are being shut down, and social media accounts are being suspended, often permanently. Governments in Europe and North America have launched numerous investigations, and in some cases have brought criminal charges (like the U.S. did against individuals involved in attempts to influence the 2016 presidential election). A flurry of new research articles, reports and books have shed light on the problems of fake social media accounts, troll farms, fake news, manipulated photos and videos, and the threats these and other things pose to the health and prosperity of a democratic society. But each of us also has an important role to play in recognizing and repelling digital influence efforts by taking personal responsibility for critical thinking and self-reflection about our biases and prejudices, while also thinking carefully before sharing or spreading information that benefits the digital influence mercenaries at our own expense.

Acknowledgments

I owe a great debt of gratitude to literally thousands of people who have significantly influenced my intellectual journal into the sordid world of digital influence mercenaries. First, I need to express my appreciation to Jacob Shapiro for his feedback and advice along the way. I have also benefited greatly from the hard work and publications of researchers like Olga Belogolova, J.M. Berger, Kate Starbird, Marc Owen Jones, Claire Wardle, Clint Watts, Barb McQuade, Cass Sunstein, Camille Francois, Carl Miller, Caroline Orr, Thomas Rid, Cindy Otis, Phil Howard, Samantha Bradshaw, Samuel Woolley, Peter Pomerantsev, Emma Barrett, Nathaniel Gleicher, Emma Briant, Erin Gallagher, Jay Rosen, Joan Donavan, Judd Legum, Natalia Antonova, Nick Carmody, and Yael Eisenstat. If you like the contents of this book, you will find the work of these people most enlightening, in addition to the hard-working folks at the Oxford Internet Institute's Computational Propaganda Project, the Global Network on Extremism and Technology, the Centre for the Analysis of Social Media, the RAND Corporation's Truth Decay project, Graphika, and the Stanford Internet Observatory. Weekly publications like *First Draft,*

Popular Information, and *The Source* (published by the Atlantic Council's Digital Forensic Research Lab) are also strongly recommended.

I sincerely thank the Naval Institute Press, particularly Senior Acquisitions Editor Pat Carlin and Director Adam Kane, for agreeing to work with me in molding this manuscript into publishable material. I also thank the anonymous peer reviewers who assisted the Press with identifying deficiencies in this manuscript that needed to be remedied before it was ready for public consumption. Any errors in facts or conceptual explanations remaining in this book are mine alone. And finally, I thank Alicia, Chloe and Jack for always being a positive influence in my life.

James J.F. Forest, Ph.D.
Lake Winnipesaukee, NH
June 1, 2021