A Villain's Guide To Social Media And Web Science

Mark Bernstein
Eastgate Systems, Inc.
134 Main Street
Watertown MA 02472 USA
Bernstein@eastgate.com

Clare Hooper
Vancouver, BC, Canada
clare@clarehooper.net

ABSTRACT

If we have not yet achieved planetary super-villainy on the desktop, it may be feasible to fit it into a suburban office suite. Social media and Web science permit the modern villain to deploy traditional cruelties to great and surprising effect. Because the impact of villainous techniques is radically asymmetric, our fetid plots are difficult and costly to foil.

CCS CONCEPTS

• **Software and its engineering→Software creation and management→Designing Software • Applied Computing→Computers in other domains.**

KEYWORDS

Hypertext, social media, literature, fiction, implementation, history of computing, politics, villainy.

ACM Reference format:

M. Bernstein and C. Hooper. 2018. A villain's guide to social media and Web Science. In *Proceedings of the 29th ACM Conference on Hypertext and Social Media, Baltimore, MD USA, July 2018 (HT2018)*, 5 pages. https://doi.org/10.1145/3209542.3210576

1 INTRODUCTION

Technological innovation has long facilitated villainy at ever greater scale. Technology, moreover, offers many opportunities to cater to the whims and caprice of the individual villain. The vandal hordes of antiquity were proverbially destructive, but they were hordes: They lacked the personal touch. More recent efforts such as the M. Ming's Gigantic Nitron Ray, D. Vader's Death Star, and A. Goldfinger's thermonuclear attack on international markets, achieved that personal touch only by commanding vast stockpiles of capital.

Previous technological approaches to villainy depended on doomsday machines, zombie apocalypses, thermonuclear devices and the like, as these were the only available technologies that supported large-magnitude calamities. Social media and Web science permit the modern villain to deploy traditional cruelties at unprecedented scale. We admit that small cruelties and local harms can be just as satisfying as global conquest, mass destruction, or summoning the elder gods. Still, there is satisfaction in numbers, and only by specifying a victim pool of adequate size can we ensure the statistical significance of our results.

The focus of this work is restricted to villainy. We are not concerned here with merely criminal uses of social media and the Web, such as money laundering, theft, or embezzlement. Similarly, we do not consider unethical practices that may not be criminal, much less villainous. Our concerns, as always, are domination of cities, nations, and planets, accumulation of wealth beyond the dreams of avarice, the destruction of dreams and widespread infliction of pain.

2 VICTIM PROCUREMENT

Social media generate vast resources of information about the interests, habits, and circumstances of millions of people throughout the world. Much information is, of course, contained in the users' posts, data they freely make available for our use. Other useful information is implicit in their use of social media to keep in touch with friends and family, to discover entertaining Web sites, or to purchase products. We can use this vast stream of data to identify those to whom we might most profitably devote our attentions. Where an advertiser looks for a persuadable and remunerative prospect, villains look for a vulnerable and satisfying victim.

It is useful in this connection to distinguish between intrinsic and extrinsic vulnerability. The intrinsically vulnerable target is subject to attack by their circumstances and context; the friendless are natural victims, of course, but so, too, are those whose friends are largely disjoint from ours. This is readily detected through the social graph [13]. Extrinsic vulnerability occurs when people have secrets: hidden families, complex love affairs, financial strain are all classic indicators, and these, too, may be detectable from social networks alone [3].

We now know it is possible to de-anonymize anonymous social graphs [2] and that private information like religious belief may be inferred from such seemingly secular statistics as Wikipedia edit counts [15]. It is essential, too, to remember that we are villains; sometimes, the old ways are the best ways, and a simple kidnapping or a short prison term can lead people otherwise

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

HT '18, July 9–12, 2018, Baltimore, MD, USA
© 2018 Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-5427-1/18/07…$15.00
https://doi.org/10.1145/3209542.3210576

hostile to us to help de-anonymize even the most obfuscated data or to give us the most closely guarded password [7] [17] [14].

Because we never give a sucker an even break, the benefits of victim identification may be considerable. Collateral benefits can be surprising and far-reaching; the persistence of Nigerian Prince or 419 scheme is ample testimony to the rewards of a villainy that surely, at this date, has vanishingly low recall. [10] Remember that a good victim is our greatest asset, that inflicting pain is good in itself, and that today's victim may be compelled to assist us tomorrow.

3 DISMAYING OUR ENEMIES

Not only can we use social media for our dark purposes and analyze it for our nefarious ends, but at the same time we can prevent our enemies from enjoying its benefits. Twenty years ago, one could send email to nearly any active computer scientist and be confident that it would be received and read; today, spam filters, phishing attacks, and ad filters make many scholars inaccessible.

Social media are exquisitely vulnerable to trolls[1], and their vulnerability is only increased when, as in Facebook, users are encouraged to combine professional, community, and personal friends in a common network. Good people can sometimes tolerate being unjustly criticized in the pages of an obscure and dusty journal; to be smeared before one's family and closest friends, on the other hand, will try the patience of saints. Helpfully, bystander apathy is the norm online [23].

Through *dogpiling*, we can exploit social networks to prevent their use by opponents. When someone makes a statement we dislike or that is adverse to our cause, we disagree and initiate a discussion. But we don't do this once: we summon dozens of friends and allies to join us simultaneously. Our victim cannot spread their message or interfere with our schemes; they must either argue with dozens of opponents or abandon the matter. Bystanders will gather to learn what the fuss concerns, and may be impressed by our apparently great numbers.

Dogpiling, moreover, is massively asymmetric. Our victim asserted something they believe and care about Perhaps their deluded friends share their misguided conviction. They were in any case writing gratuitously, describing their thoughts to their friends. We, however, are villains: well-paid professionals with an interest in hounding them and in winning. We may easily employ assistants (*minions*) to add their voice to ours; a single minion can engage in many arguments at once, and can control numerous separate personae and supervise dozens of autonomous 'bots. Our opponents may care deeply, but our minions suffer no corresponding handicap: win or lose, the minion gets paid [20].

Though most minions require minimal skills and training, it is sometimes possible to acquire minions who are already well placed in social networks. These can be invaluable for dogpile attacks, as they lend not merely their own weight but also the mass of their followers. Recruitment to our wicked cause is facilitated as well by the observation that the online world is a place where people "just like to be nastier" [22]."

We must also remember that conventional villainy may be employed with profit on the social media battlefield. Blackmail, for example, may effectively silence even the most influential and experienced Wikipedia opponent. Elaborate and inconvenient security arrangements can be defeated by simply accosting the target and displaying a weapon. Indeed, speculating about attacking a pet animal may suffice, not only from fear of losing the services and cost of the target's mangy little dog, but because the target will understand that if villains knows about Toto, they also know details of the rest of their beloved circle. Crowd-sourced research can frequently reveal surprising insights into an anonymous writer's life[4], and these may be deployed through conventional means among the target's family, employers, and neighbors. Sometimes, we can sit back and enjoy the fun while the asymmetries of public outrages and confusion do our work for us[1].

4 MINING

Great efforts have been dedicated to anticipating individual needs by mining users' online behavior, since advertising will naturally be most profitable when directed to those who already need the advertised goods. It may be possible for algorithms to detect needs and desires before they are consciously expressed — for example, to detect from her purchasing and browsing behavior that a woman may be pregnant before she (or her family) knows [11]. Might it be possible to identify women who will soon seek to terminate a pregnancy prior to conception? Even accepting a substantial error rate, great mayhem might be achieved at very little cost. Similar mining efforts directed at other behaviors — romantic entanglements, dread diseases — could yield spectacular dividends [8]. Powerful and well-established methods can reliably trick people into revealing more than they intend [24]. The online world is our oyster.

Again, we observe a pronounced asymmetry in the villainous effects of data mining. Our opponents must make do with data that they can access freely or that they can purchase. Unlike them, we are free to use stolen data — either information that happens to have been stolen (John Podesta's emails, Vermeer's *The Concert*), or information whose theft, being advantageous to our plans, we commission. Co-occurrence in large, stolen data stores can be a powerful tool in itself; a cluster of healthy, athletic users of watch-based fitness apps who are geolocated in an area that is blank in Google Maps may be a secret military base [12]. Analysis of big data thrives on bigger data: our data will always be bigger than theirs, and we can buy, borrow, and steal more.

5 STEALING CANDY FROM A BABY

Although we now enjoy unprecedented computational power and can employ analytical tools that exceed the wildest dreams of our predecessors, it behooves us to remember the simple joys of those bygone days. Let us consider, for example, stealing candy from a baby. Nothing could be easier to contemplate or swifter to accomplish. Yet, through a single act, we reap many benefits.

- The baby is wretched, naturally, and expresses its dismay with appropriate force.

[1] http://www.cbc.ca/news/canada/calgary/jeremy-quaile-knightley-dog-death-calgary-1.4602948

- An infant's cry of distress cannot be resisted: its parents must stop what they were doing, however virtuous and important their plans may have been, to attend to the child.
- Bystanders will be annoyed and distracted, and may cast disparaging glances at the parents who permit such disruption. Discord is sown.
- The infant may have siblings; if so, they may be jealous of the attention the baby is receiving, and may take advantage of parental distraction to engage in roughhousing, casual vandalism, or indoor parkour practice.
- And, you get a lollipop!

The intent of this perfidious pastorale is not to indulge nostalgia for a simpler era, but to observe the powerful asymmetry we can so gainfully employ. To steal candy from a baby is proverbially easy, yet the theft does not merely please the thief and dismay the baby; parents, siblings, bystanders, the owners of the candy shop, the paramedics summoned when indoor parkour practice goes awry, all share and multiply the impact. Efforts to foil our scheme are disproportionately difficult: for example, handing out free lollipops to passing infants is unlikely to exert an equal effect.

Social networks exploit network effects. Not only do the asymmetric effects of villainy benefit the same network phenomena, but the villainy also benefits the social network. On the internet, wronged innocents wail online, and their cries attract clicks (which improve the platform's stock valuation) and viewers (to whom advertising may be displayed). Crowds that gather at the crime scene are themselves famously vulnerable to villainous exploitation [9]; a modest expenditure of effort and resources can keep an event like Gamergate or Pizzagate in play for weeks or months. Virtuous peacemakers diminish platform profits.

Analyzing the crowds gathered by these events may yield useful leads for staffing your malevolent enterprises. Conventional global villainy once entailed a large and costly staff of mad scientists and renegade warlords. These indispensible personnel were costly to hire and difficult to manage. Our armies of minor minions, moreover, required salaries, training, and the acquisition of at least the same number of cool uniforms, while a costly Human Resources division was needed to locate and recruit them. Though villains were pioneers in employing the physically challenged [16], those challenges brought expense, inconvenience, and sometimes betrayal [20]. Much recruitment and support can now be automated; indeed, minions often appear at our crime scenes and volunteer for service. Others, observed committing spontaneous villainies at the scene of your own crimes, can be recruited with ease. Within minutes of the Parkland, Florida school shooting, for example, 8chan chatboards were filled with efforts to coordinate stories to blame the reaction to the crime on Jewish kabalistic numerology and hired crisis actors [21]. Many of our most technically-demanding roles may now be crowdsourced.

Nor should we neglect the costs of maintaining entire districts to serve as vile dens and wretched hives of scum and villainy. Now, we can recruit minions in their own basements to support our repellent endeavor. They advance our dark ends without costly secret bases or inconvenient hidden fortresses.

6 DISINFORMATION AND DISCORD

What is better than making one's fellow man believe something that is not true? Why, making vast numbers of people believe something that is both preposterous and harmful! Systematically spreading false news has proven to be of enormous value.

Familiar analytical techniques for real-time sentiment analysis and A/B testing can now be deployed to track engagement and propagation of false information. We can know within minutes what messages are most attractive to different audiences. A single weird trick may be sufficient to capture the imagination of niche audiences through hyper-tailored, adaptive messaging. Our successes are our own; our failures cost us nothing.

Engagement aroused by provocative and targeted false news benefits us. Our opponents are bound to try to discredit the news; their futile struggles only increase our reach. Discourse generation and assistive writing tools allow minions with limited skills to manage numerous online personae, each of which can contribute to spreading our message. A single semi-literate minion can, in favorable circumstances, engage several distinguished professors and authoritative pundits. Because many of the bystanders witnessing the argument will undoubtedly resent teachers — who among us has no desire to avenge old classroom wrongs? — our minion may well achieve surprising success. Yet even if our minion is vanquished and today's message is entirely discredited, no harm is done; our minion can go home, drink a beer, enjoy a good cackle with friends, and tomorrow our minion can pick up its new followers, put on a new persona, and try again. The more we engage, the more traffic we receive.

There are a million lies in the naked city, and only one truth. Our sanctimonious rivals will fight endlessly among themselves to define and refine that truth, even if the result is adverse to their personal and political interest. While they parse nuance and endure inconvenient truths, we invent our own, numerous truths and test them rigorously for efficacy. What is more, we design our untruths to be more interesting than truth, and so our foul fantasies will be shared and retweeted far more frequently than truthful reports[25].

Disinformation promotes discord. We consider discord good in itself, of course, but discord also weakens our opponents while strengthening our other operations. Our truthiness itself promotes further discord among our enemies, as each invidious invention demands provokes a new fissure among our fractious enemies.

Disinformation has revived some of our oldest aspirations, villainous visions once thought lost forever. The dream of a single vast database that identifies every prominent Jew (as defined by the *Nürnberger Gesetze!*) once seemed lost forever, but numerous Wikipedia efforts labor daily to make it real. Wikipedia editors — often the same editors — work to render articles about marginal extremists more prominent and palatable, to excuse (and publicize) racist and anti-Semitic memes, and to defame both contemporary and historic figures. Deliberate campaigns to move the Overton window target topics such as Nordic Nazi Parties; if Sweden and Norway have white supremacists, they argue, perhaps Nazism is worth a second look?

7 RELATED WORK

Though early villainy was sometimes conceived at surprising scale (see *Paradise Lost*, or the *Prose Edda*), it was only after James Moriarty's invention of organized crime that technology could properly be applied to our ends. The early work of Sauron is typical in its acceptance of the limitations of scale, targeting a mere nineteen initial victims: as the nineteen designated targets were the rulers of the known world, the scheme did demonstrate commendable audacity. Computational efforts to summon the elder gods [18], to mock creation [16][21] or to bring on the end of the universe [6] anticipate the approaches described here.

Preliminary efforts known as Gamergate, though unsuccessful in reforming ethics in game journalism, did succeed in harming a handful of targeted victims while requiring our opponents to expend thousands of hours in order to oppose our handful of amateur villains. The same methods are generally believed to have been applied to the 2016 US Presidential Election with surprising success.

Villains may learn a great deal from well-intentioned systems. When Facebook, for example identified images that might evoke fond memories of the preceding year and urged people to share them with their social networks, it showed Eric Meyer the portrait of his six-year-old daughter who had recently succumbed to aggressive brain cancer [19]. "Yes, my year looked like that. True enough," he wrote. "My year looked like the now-absent face of my Little Spark. It was still unkind to remind me so tactlessly." Another well-intentioned Facebook feature proposed new candidates for admission to each user's social network, demonstrating a surprising facility at proposing the user's former romantic partners.

8 CONCLUSION

Much though we deplore the fact, technological progress can benefit the virtuous as well as the evil. What seems striking in this brief and anecdotal survey of new techniques and recent developments are the prominent asymmetries that redound to the benefit of villainy.

- The villain can lie, the good should not. Disinformation is villainous in itself and leads to discord, which is even better.
- The villain can steal, the good must not. Data mining is powerful, but its power increases as more data becomes available. Our neural networks do not care that some of our data is stolen.
- Disinformation and rumor may be spread by the idle, the unskilled, and the robot. To confound them requires the attention of skilled advocates.
- We can choose the lies that serve us best; our enemies cannot. There are a million lies but only one truth.
- A working minion, stymied, can dust itself off and work on a new meme. A true believer in the same position may experience profound humiliation.
- A single scurrilous word or damaging disclosure can do lasting harm that a thousand well-intentioned and sympathetic notes will not repair.

ACKNOWLEDGMENTS

This is a satire. Don't try this at home. The works cited here are not villainous. We don't know the Twitterological literature as well as we ought, and any apparently-inexplicable choice to single out a particular research effort is surely due to our ignorance. We thank David E. Millard, Charlie Hargood, Dr. Fionnbar Lenihan and Robert A. Sullivan for helpful conversations on related topics. Of course, none of them are in any way responsible for this villainous paper.

REFERENCES

[1] Ammann, R. 2009. "Jorn Barger, The Newspage Network And The Emergence Of The Weblog Community," Proceedings Of The 20th ACM Conference On Hypertext And Hypermedia". *HT '09.* 279-288.

[2] Backstrom, L., Dworkin, C., and Kleinberg, J. 2011. "Wherefore Art Thou R3579x?: Anonymized Social Networks, Hidden Patterns, And Structural Steganography". *Commun. ACM.* 54, 12, 133-141.

[3] Backstrom, L. And Kleinberg, J. 2014. "Romantic Partnerships And The Dispersion Of Social Ties: A Network Analysis Of Relationship Status On Facebook Proceedings Of The 17th Acm Conference On Computer Supported Cooperative Work \&\#38; Social Computing". *CSCW '14.* 831-841.

[4] Johnson, B. 2001. "The Short Life Of Kaycee Nicole". *The Guardian.*

[5] Chen, A. 2015. "The Agency". *New York Times Magazine.*

[6] Clarke, A. C. 1967 *The Nine Billion Names Of God; The Best Short Stories Of Arthur C. Clarke.* Harcourt, Brace & World.

[7] Derakhshan, H. 2016. "Killing The Hyperlink, Killing The Web: The Shift From Library-Internet To Television-Internet Proceedings Of The 27th Acm Conference On Hypertext And Social Media". *HT '16.* 3-3.

[8] Dick, P. K. 2016 *The Minority Report : And Other Classic Stories.* Citadel Press.

[9] Dickens, C. 1870 *The Adventures Of Oliver Twist.* Fields, Osgood & Co.

[10] Edwards, M., Peersman, C., And Rashid, A. 2017. "Scamming The Scammers: Towards Automatic Detection Of Persuasion In Advance Fee Frauds Proceedings Of The 26th International Conference On World Wide Web Companion". *WWW '17 Companion.* 1291-1299.

[11] Hamilton, D. 2016 *The Thinking Machine.* In Echoes Of Sherlock Holmes : Stories Inspired By The Holmes Canon, L. R. King, L. S. Klinger, J. Connolly, M. Gardiner, D. Cameron, T. Alexander, D. Morrell, T. Lee, B. Musson, H. P. Ryan, A. Perry, M. Scott, H. Ephron, G. Phillips, W. K. Krueger, C. Mcpherson, D. Crombie, J. Maberry, D. Mina, And C. Doctorow, Eds. Pegasus Books.

[12] Hern, A. 2018. "Fitness Tracking App Strava Gives Away Location Of Secret Us Army Bases". *The Guardian.*

[13] Huang, Q., Singh, V. K., And Atrey, P. K. 2014. "Cyber Bullying Detection Using Social And Textual Analysis Proceedings Of The 3rd International Workshop On Socially-Aware Multimedia". *SAM '14.* 3-6.

[14] Le Carré,, J.. 1980 *Smiley's People.* Knopf.

[15] Rizoiu, M.-A., Xie, L., Caetano, T., And Cebrian, M. 2016. "Evolution Of Privacy Loss In Wikipedia Proceedings Of The Ninth Acm International Conference On Web Search And Data Mining". *WSDM '16.* 215-224.

[16] Shelley, M. W. 1984 *Frankenstein, Or, The Modern Prometheus.* Modern Library.

[17] Sofia El Amine, S. B., Sabrine Saad, Addis Tesfa And Christophe Varin "Infowar In Syria: The Web Between Liberation And Repression". *Web Science 2012.*

[18] Stross, C. 2006 *The Jennifer Morgue*. Golden Gryphon Press.

[19] Meyer, E. 2014 "My Year Was Tragic. Facebook Ambushed Me With a Painful Reminder**.**" *Slate*, http://www.slate.com/blogs/future_tense/2014/12/29/facebook_year_in_review_my_tragic_year_was_the_wrong_fodder_for_facebook.html

[20] Czege, P. *My Life With Master*, Half-Meme Press, 2003.

[21] Timberg, C. and Harwell, D. 2018 "We studied thousands of anonymous posts about the Parkland attack — and found a conspiracy in the making", *The Washington Post* (28 February 2018)

[22] Nevin, Andrew D. 2015. *Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct*. M.A. Thesis, Western University. https://ir.lib.uwo.ca/etd/2926

[23] DiFranzo, D., Taylor, S. H. et al., 2018, "Upstanding by Design: Bystander Intervention in Cyberbullying", *CHI 18* (Montréal 21-26 April 2018)

[24] Brignull, Harry. "Types of Dark Patterns," https://darkpatterns.org/types-of-dark-pattern

[25] Vosoughi, S., Roy, D., and Aral, S. 2018 "The spread of true and false news online' *Science* (9 March 20-18) pp. 1146-1151