Black Hat Trolling, White Hat Trolling, and Hacking the Attention Landscape

Matthew Goerzen
Data & Society Research Institute
New York, NY, United States of America, matt@datasociety.net

Jeanna Matthews
Department of Computer Science
Clarkson University, Potsdam, NY, USA, jnm@clarkson.edu

ABSTRACT

In this paper, we analogize the practice of trolling to the practice of hacking. Just as hacking often involves the discovery and exploitation of vulnerabilities in a computer security landscape, trolling frequently involves the discovery and exploitation of vulnerabilities in a media or attention landscape to amplify messages and direct attention. Also like with hacking, we consider the possibility for a range of trolling personas: from black hat trolls who push an agenda that is clearly counter to the interests of the target, to gray hat trolls who exploit vulnerabilities to draw critical attention to unaddressed issues, and white hat trolls who could help proactively disclose vulnerabilities so that attack surface can be reduced. We discuss a variety of trolling techniques from dogpiling to sockpuppetry and also a range of possible interventions.

KEYWORDS

Trolling, hacking, media, ethics, politics, memes, journalism, media governance, social media

ACM Reference format:

Matthew Goerzen and Jeanna Matthews. 2019. Black Hat Trolling, White Hat Trolling, and Hacking the Attention Landscape. In *Proceedings of WWW '19: The Web Conference (WWW '19), May 13, 2019, San Francisco, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3308560.3317598

1 Introduction

In the early days of the Internet, users adopted the fishing term "trolling" to describe duplicitous postings designed to lure readers into engagement or reaction. While typically understood as a form of deceptive entertainment [1], the activity was also intelligible as a mode of governing other users, especially new users, in the Usenet discussion groups where the behavior was first documented [2]. A common pattern was for a veteran user to introduce a controversial topic that had been so extensively addressed in the past that only a new user would respond earnestly to the post. Other veteran users would know that the topic was a "troll," but new subscribers to the group would not--and thus might be baited into an extensive response, revealing their ignorance. This type of trolling could serve to identify "newbies" from group insiders and generally enforce community norms.

The concept of trolling has expanded to include a much wider range of behavior, from imageboard users raiding for "lulz" [3] [4], to hacktivists drawing media attention to activist causes [5], to state-sponsored propaganda and influence operations [6] [7] [8]. Trolling is often associated with online harassment, abuse, and disruption—especially with political or ideological intent [9] [10]. Trolls use controversy to sow chaos and amplify disinformation, bait journalists into reporting false information, and generally attempt to manipulate popular opinion [11]. But the label has also been applied to artists and online activists who exploit media dynamics to draw critical attention to the workings of socio-technical media systems [12] [13].

In this paper, we seek to frame trolling as the hacking of our shared media or attention landscape. We can view mass media and social media platforms as socio-technical systems to be secured. Through this lens, we argue that much like hacking often involves the discovery and exploitation of vulnerabilities in a computer security landscape, trolling typically involves the discovery and exploitation of vulnerabilities in our media or attention landscape. danah boyd has described activity of this kind as "hacking the attention economy" [14], while Rand Waltzman has called for "cognitive security" to address this mode of activity [15]. Most recently, Bruce Schneier and Henry Farrell have suggested expanding the scope of computer security to address "soft cyber" attacks such as politically-motivated trolling [16]. Attention hackers or trolls attempt to set the media agenda, directing journalists, social media users, and others to information that serves their interest. Often their techniques emulate or take advantage of platform dynamics designed to benefit advertisers and data-centric enterprises [17] [18]. The changing media landscape of mass media, social media, and algorithmic curation constantly introduces new vulnerabilities for attention hackers to exploit.

WWW '19, May 13, 2019, San Francisco, USA

ACM ISBN 978-1-4503-6675-5/19/05.
https://doi.org/10.1145/3308560.3317598

2 Trolling Techniques

In Table 1, we list various trolling techniques. In most trolling techniques, a piece of disinformation is introduced as bait for a target or victim to ingest. The troll is typically looking for the target to take the bait and produce a reaction that will be observed by others. Often, the third-party observers or interpreters are meant to recognize the naivety of the target in accepting the bait as legitimate. The intended outcomes can vary from simply trying to embarrass the victim to provoking a particular political objective.

Table 1: Selected Trolling Techniques

Name	Description
Source Hacking / "Journobaiting"	Planting false claims or posing as sources to dupe mainstream media, especially in the wake of a crisis event.
Keyword Squatting	Associating a rarely used keyword or search term, especially one that becomes suddenly popular in the wake of a crisis event, with disinformation or propaganda.[a]
Denial of Service	Overwhelming a public space with information or data designed to promote exhaustion and disaffection, or generally frustrate sensemaking efforts.[b]
Sockpuppetry	The creation and management of social media accounts designed to appear as authentic individuals, typically using "data craft."[c]
Persona Management / Botherding	The co-ordination of multiple sockpuppet accounts or their algorithmic automation as a botnet.
Ironic Hedging / Bait and Switch	Using hateful or extreme language and imagery in a way that creates plausible deniability about intent and empowers messagers and some interpreters to downplay sincerity and seriousness.
Political Jujitsu	Soliciting attack from an opponent to elicit sympathy from political allies, ground victimization narratives, facilitate recruitment, and justify counterattack.
Controlling the Opposition	Using sockpuppet accounts to pose as representatives of an oppositional group.
Astroturfing	Using sockpuppet accounts to create the illusion of a bottom-up social movement or social outcry.
Wedge Driving	Inserting narratives designed to create divisive infighting among social groups. Often part of an overarching "divide and conquer" strategy.
Memetic Trojan Horses	The popularization of seemingly banal content that opens the Overton Window [d] by prompting commentary from mainstream journalists.
Deep Fakes [e]	Altering photographs and videos to change the original message, in a way that is difficult to detect.
Concern Trolling	Disingenuously expressing concern about an issue in order to derail discussion and damper consensus. Posing as a concerned ally or objective third party in order to make criticisms more palatable.
Brigading / Dogpiling	Bombarding a targeted individual or space with ad hominem attacks from multiple accounts.[f]
Conspiracy Seeding	Spreading "breadcrumbs" on social media and anonymous forums to nudge participants towards conspiracist thinking.
Algorithmic Gaming	Exploiting the functioning of an algorithm or related databases to elicit a result not intended by its designers. [g]

[a] This often involves SEO techniques, but can also involve the brute force appropriation of hashtags.

[b] The Grugq has described the release of a data trove of purportedly damaging information about Emmanuel Macron immediately before the 2017 French presidential election media blackout in these terms, as a "Data Denial of Service Attack" [19].

[c] "Data Craft" is the term used by Amelia Acker to describe the manipulation of metadata (geolocation, follower count, etc.) to enhance the authenticity of a fake social media account [20].

[d] The Overton Window refers to the range of political ideas available for address in public discourse.

[e] The term Deep Fakes comes from a subreddit devoted to producing videos using GAN techniques. It's come to stand in for a variety of image

manipulation techniques, including manual photoshopping—or what used to be called "shops."

[f] It should be noted that a number of individuals have pushed back on the idea that targeted harassment or abuse be described as "trolling," noting that the terms harassment and abuse already describe this behavior [21] [22]. However, we believe the prevalence of these techniques in subcultural trolling communities warrants their inclusion in this inventory.

[g] Of course, this raises questions about whether designer intent matters—i.e., whether an affordance is a "bug" or a "feature" and who gets to decide [23].

Trolls are often motivated to achieve specific political objectives. They may seek to draw attention to ignored issues ("agenda setting") or alternatively to waste attention and distract from issues. They may seek to pressure politicians, consumers, voters, businesses, or bureaucrats into action by shaping public attention, or they may attempt to draw a telling response as a way to increase transparency and accountability. They may wish to diminish an opponent's resources or morale, perhaps to exhaustion (e.g. by promoting "outrage fatigue" or dumping vast swathes of data, effectively "denying service"[1]). Some trolls seek to raise skepticism or to tear down all accepted sources of authority. Others simply want to cause trouble for the fun of it (lulz). Trolling can be done, as in the early Internet, to enforce community standards as a form of community building or governance, or to provoke deliberation regarding community norms.

Trolling can be surreptitious, but most trolling involves a revelatory moment where the deception is revealed or discovered, and the troll recognized. Common targets of trolling are journalists (and their readers), social media users (both allies and potential allies, and those perceived as opponents), companies, politicians, and regulators.

3 Vulnerabilities in Our Attention Landscape

In computer security, vulnerabilities are most often discussed in relation to technical systems like software code, hardware design, or network configurations and protocols.[2]

To consider where vulnerabilities lie in relation to trolling it is helpful to consider socio-technical systems. Here, vulnerabilities can present at multiple levels, typically where technical design overlaps with economic incentives, organizational factors, political objectives, and even psychological factors like cognitive bias. For our purposes, we will consider mostly social media, legacy news media, and the communities they service as the socio-technical systems particularly vulnerable to trolling.

In relation to news media, we can consider how a long-standing editorial predilection for novel, salacious, and spectacular content ("if it bleeds it leads") creates opportunities for trolls to bait journalists and set media agendas from below. We could also consider how editorial vulnerabilities have been exacerbated by the always-on, breaking news environment of continual online publishing and the competition for social media click-throughs. More complex to reckon with is the way many digital first media organizations themselves troll for user engagement through the production of "clickbait" headlines designed to circulate and capture attention on social media platforms.

Social media platforms have introduced new vulnerabilities due to their reliance on automated amplification and curation. For example, attention hackers can amplify their messages through the creation of bots that simulate the signs of organic human interest in a topic (e.g. liking, following, sharing, forwarding), or by reverse engineering algorithmic processes in order to game them. Understanding the metadata associated with messages and the ways in which online social media platforms use this metadata to decide which messages to amplify is key to identifying vulnerabilities that trolls can exploit [20]. In general, the anonymity available in many social media platforms offers both vulnerabilities and affordances for the amplification of messages.

Taking a broader scope, we could consider also that most forms of media or attention amplification systems harbor a critical vulnerability that exacerbates other vulnerabilities: the asymmetric cost to debunk false information. False, inflammatory, and hyper-partisan information may spread quicker than factual information, garner more attention, and be remembered longer [24] [25] [26]. Furthermore, attempts to debunk false information can unintentionally direct more attention and may counter-intuitively lead more people to believe the false information [27] [28].

Another example of a broad socio-technical vulnerability is "Poe's Law," a phenomenon named after Nathan Poe in 2005 when he observed that it is impossible to create a parody of extreme views so obviously exaggerated that it cannot be mistaken by some readers for a sincere expression of the parodied views [29]. Poe's Law can be exacerbated by design decisions (such as user anonymity) and more complex emergent factors (like "context collapse," where a publicly shared message intended for one audience is interpreted differently by another [30]).

In general, the economics of the ad tech economy and the ways in which algorithmic curation happens in online platforms is a source of many new vulnerabilities. For example, whenever a platform has not accumulated substantial history on a topic or search term, it is vulnerable to malicious actors dictating the output of the system [31]. Similarly, the economics of revenue for clicks can drive the creation and spread of divisive, false, and extreme content [32]. Nation-state actors have even created weaponized social media infrastructure for message amplification, that in many contexts swamps the organic signal of human discourse [33].

Considering all these examples, we can recognize that socio-technical vulnerabilities can appear in multiple places and at multiple scales. Some might consider that the entire existence of a platform like Facebook constitutes a vulnerability to the broader sphere of human interaction. Others might consider the

1 As Darin Barney has noted, excess information—even of an overtly political salience—can have a depoliticizing effect [45].

2 Of course, there are exceptions: organizational threat modeling often considers the impacts of social engineering attacks or the "human element," and many hacktivists advocate for a higher order conception of security aligned with human rights frameworks.

platform banal or even beneficial, but see the platforms policies around data enclosure and shareholder value as creating perverse incentives for its designers and advertisers. Others might consider that specific design features of Facebook—like the way its algorithms curate information—constitute vulnerabilities that ought to be fixed. Others still might suggest that only design features that do not work as intended constitute vulnerabilities. And still others might find fault with its content moderation policies. Determining what is a "bug" and what is a "feature" can often be subjective—and such judgment likely depends on an evaluator's propensity to benefit from the issue at hand.

4 Black Hat, Gray Hat, and White Hat Trolls

Within the computer security community, a clear distinction is made between black hat hackers who exploit computer systems to cause harm or generate profit for themselves and white hat hackers who exploit computer systems in order to proactively discover vulnerabilities that could be patched. We would like to propose a similar distinction for trolling.

A black hat troll could be understood to push a private agenda on their own that is counter to target's interests and counter to accepted standards of community governance. A white hat troll could be understood to identify, document, and reveal vulnerabilities selectively to platforms so as to reduce their attack surface and help align media systems and platforms with designer intent.

Black hat trolls would typically be using forms of engagement that are not prescribed by the designer of the system and white hat trolls would be looking for ways to disable forms of non-prescribed engagement through research and education.

Again, as with hackers, we further envision a category of gray hat trolls that use non-prescribed methods of engagement, but are motivated by a sense of public interest rather than an intention to harm or secure personal gain. They may view their actions as a way to demonstrate attack surfaces and thus increase pressure on gatekeepers to change their systems, or as a form of "hacktivism" that exploits the vulnerabilities of a system to further a perceived higher order goal of advocating for human rights or "human security."

White hat and gray hat trolls could perform penetration testing, engage in security research, and disclose vulnerabilities. They could also intervene by identifying bad actors, their incentives, and their methods. Furthermore, white hat and gray hat trolls might actively "troll back" or counter bad actors by "trolling the trolls."

The varied methods deployed by white hat hackers, black hat hackers, and gray hat hackers have inspired tremendous controversy in the computer security community—as debates around the full disclosure movement, hacktivism, bug bounty programs, and "hack back" policies can attest [34] [35] [36] [37], but these debates have also contributed to the establishment of functional computer security institutions. By schematizing trolling activities in this way, we could anticipate the generation of similarly productive debate regarding the ethics of trolling and the governance of socio-technical systems like social media platforms.

5 Amplification and the Design of Media Platforms

Defending against trolling requires consideration of acceptable forms of message amplification. For much of the history of 20th century pre-digital media, journalists and other mainstream media gatekeepers followed professional codes of ethics which typically included commitments to the accuracy of information, verification of sources, and the fair representation of multiple sides of an issue [38]. However, in practice these ethics are not always followed or enforced. And even when journalists operate within the bounds of these frameworks, they may be incentivized by thought of money, fame, power, political interest, or expertise to unduly amplify advantageous messages. Moreover, the same incentives can lead them to leave potentially important messages unamplified and under-represented.

Social media offered the promise of more democratized amplification of messages. However, in an information system in which anonymity can lead to multiple "votes" per person, we have encountered an emergent set of problems. Someone may have the right to free speech with their one mouth and body, but do they have the right to 20000 bots to amplify their message? Do they have the right to use sockpuppet to caricature those on the other side of an issue in a way that makes them appear ridiculous or extreme? When attention is scarce, does monopolization of attention by some constitute a denial of service attack on the rights of others' speech and an attack on the "attention sovereignty" of the limited attentional resources of individuals?

We have to grapple with the fundamental question of how we decide which messages should be amplified, and how best to gauge and represent "public opinion"—questions that have long concerned mass communications and journalism scholars, and only emerge anew in an era of "networked gatekeeping" [39]. Some have argued that the answer is educating individuals about fact checking and media literacy. However, is it really feasible for every individual to function as an investigative journalist, rigorously interrogating all claims that come into their media feeds? No one has the resources to verify/investigate every claim. When inflammatory lies are stickier and more profitable than real facts, it is difficult to imagine that fact-checking and individual action will be sufficient.[3]

If we believe that some form of gatekeeping collective attention will be necessary, then what kind? Human editors, algorithmic moderation? A preference for gatekeeping by automated systems guided by algorithms can lead to the overrepresentation of messages pushed out by those actors who have discovered ways to manipulate those systems in their favor. However, human gatekeepers, such as editors and content moderators, have demonstrated their own failings, blind spots, and incapacities. With the centralized human gatekeeping or

[3] Moreover, notions of "media literacy" may differ between different epistemic communities [40]

editing that was the norm in pre-digital mass media, ideas that emerged from marginalized communities and other disenfranchised groups often went completely unrepresented in mainstream mass media. We could consider the possibility of smaller communities selecting their own trusted gatekeepers. However, this kind of decentralized gatekeeping can lead to tribalism, where certain groups amplify fundamentally different messages from one another and lack the shared discursive objects that make co-operation and mutual understanding possible. We increasingly find ourselves in a world where different publics cannot even agree on the facts of our world, let alone align their opinions about those facts.

In the face of this fraught situation, a variety of possible interventions have nonetheless presented themselves. Below we identify a brief selection of possible top-down interventions and bottom-up interventions.

5.1 Top-down Interventions

There have been substantive discussions about the ways in which social media platforms like Twitter and Facebook could be improved (and possibly even regulated). Banning accounts that exhibit clear signs of algorithmic control (bots) is one way to reduce amplification through automation. However, this is only one source of manipulation. Disrupting economic incentives that reward click-through traffic on "fake news" or incentivize engagement for engagement's sake through regulation could be another important step [17]. Introducing additional hurdles for trust and verification of accounts (real-name policies, linking accounts to phone numbers or credit cards) is possible, but would also introduce a chilling of legitimate anonymous speech. Another category of top-down intervention could be considered "strategic silence," in which those individuals with editorial and editorial-like power in media and platform companies actively seek to avoid amplifying disinformation or even addressing it, to avoid generating more attention [27]. The user experience of a variety of platforms could benefit from the experimentation with different content moderation strategies [41]. Finally, enhanced transparency regarding moderation and amplification policies could promote good will among users, and reduce the opportunity space for political actors to claim victimization or unfair treatment. Of course, transparency on such matters could also enable those looking to brush up against the limits of acceptability as they manipulate or game platform dynamics.

5.2 Bottom-up Interventions

Not all interventions need to come from platforms or more traditional media gatekeepers. There are also a range of possible bottom-up interventions, including P2P moderation techniques like white lists and peer curated feeds. Users could introduce "countermemes" such as Godwin's Law to redirect online conversations [42], and promote active refusal to engage with disruptive influence ("don't feed the trolls") as a normative practice. Opting out of platform use is one possibility, but as many existing socio-technical media systems become increasingly integral to work and public life, both non-participation and early adoption of an emerging alternative could pose significant disadvantages to an individual [43] [44]. Users can collaborate to report content they see as negative for their community, effectively providing platforms with a rationale for removing content. Doxing those at the source of disinformation and shaming those that spread disinformation can also function as forms of community policing. Yet as stated previously, these techniques could further support the emergence of tribalism, and can themselves serve as modes of abuse or repressive gatekeeping.

6 Summary

In this messy modern world of message amplification, we see substantial benefit in understanding the history and techniques of trolling and how they serve to introduce and amplify messages. We see a role for white hat trolls to help platforms and media gatekeepers identify attacks and reduce their attack surface. We also see a role for gray hat trolls to point out vulnerabilities in the current media landscape, and to locate responsible parties and pressure them to change. If we want to see the benefits of the democratizing force of new media to amplify overlooked and under-represented voices, then we need to find ways to avoid the denial of service that comes from the manipulation of the processes and institutions responsible for gatekeeping and curating of our information environments.

7 ACKNOWLEDGMENTS

Thanks to Data & Society Research Institute for supporting this work.

REFERENCES

[1] J Donath, 1998 Identity and Deception in the Virtual Community, in Communities in Cyberspace. P Kollock and M Smith (Eds.). Routledge, London, England.
[2] M Tepper, 1996 Usenet Communities and the Cultural Politics of Information, in Internet Culture. David Porter (Ed.). Routledge, New York, NY, USA.
[3] G Coleman, 2012 Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle, in The Social Media Reader. New York University Press, New York, New York, USA.
[4] W Phillips, 2015 This Is Why We Can't Have Nice Things. MIT Press, Cambridge, Massachussets, USA.
[5] G Coleman, 2014 Hacker, Hoaxer, Whistleblower, Spy. Verso, London, England.
[6] SC Woolley and PN Howard (Eds.). 2018. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media (Oxford Studies in Digital Politics). Oxford University Press, Oxford, England.
[7] JC Ong and JVA Cabañes, 2018 Architects of Networked Disinformation. University of Leeds.
[8] C Paul and M Matthews, 2016 The Russian "Firehose of Falsehood" Propaganda Model. Rand Corporation.
[9] S Herring, K Job-Sluder, R Scheckler, and S Barab. 2002 Searching for Safety Online: Managing "Trolling" in a Feminist Forum. The Information Society, 18(5), 371-384.
[10] K Mantilla, 2015 Gendertrolling: How Misogyny Went Viral. Praeger, Santa Barbara, California, USA.
[11] A Marwick and R Lewis, 2017 Media Manipulation and Disinformation Online. Data & Society Research Institute.
[12] L Knuttila, 2016 Trolling Aesthetics: The Lulz as Creative Practice (Dissertation). York University, Toronto, Ontario, Canada.
[13] M Goerzen, 2016 Critical Trolling (MA Thesis). McGill University, Montreal, Québec, Canada.
[14] d boyd. 2017 Hacking the Attention Economy. Points blog, Data & Society Research Institute.
[15] R Waltzman. 2017 The Weaponization of Information. US Senate Testimony, Rand Corporation.
[16] B Schneier and H Farrell, Common Knowledge Attacks on Democracy. Berkman Klein Center Research Publication No. 2018-7.

[17] A Nadler, M Crain, and J Donovan. 2018 Weaponizing the Digital Influence Machine. Data & Society Research Institute.
[18] JA Braun and JL Eklund. 2019 Fake News, Real money: Ad Tech Platforms, Profit-driven Hoaxes, and the Business of Journalism. Digital Journalism, 7(1), 1–21.
[19] T Grugq. 2017 A Last Minute Influence Op by Data DDOS. Medium.
[20] A Acker. 2018 Data Craft: the Manipulation of Social Media Metadata. Data & Society Research Institute.
[21] J Bartlett. 2014 OG Internet Trolls are Upset their Hobby's Been Ruined. Vice.
[22] W Phillips. 2016 Donald Trump is Not a Troll. Slate.
[23] M Wolf, K Miller, and F Grodzinsky. 2017 Why we should have seen that coming: comments on Microsoft's tay 'experiment,' and wider implications. SIGCAS Comput. Soc. ACM SIGCAS Computers and Society, 47(3), 54–64.
[24] S Vosoughi, D. Roy, and S. Aral. 2018 The spread of true and false news online. Science, 359(6380), 1146-1151.
[25] M Sally Chan, CR Jones, KH Jamieson, and D Albarracín. 2017 Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation. Psychological Science, 28(11), 1531–1546.
[26] A Friggeri, L Adamic, D Eckles, and J Cheng. 2014 Rumor Cascades. In Eighth International AAAI Conference on Weblogs and Social Media.
[27] W Phillips. 2018 The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators. Data & Society Research Institute.
[28] J Donovan and d boyd. 2018 The Case for Quarantining Extremist Ideas. The Guardian.
[29] SF Aikin. 2013 Poe's Law, Group Polarization, and Argumentative Failure in Religious and Political Discourse. Social Semiotics, 23(3), 301-317.
[30] AE Marwick and d boyd. 2011 I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience. New Media & Society, 13(1), 114-133.
[31] M Golebiewski and d boyd. 2018 Data Voids: Where Missing Data Can Easily Be Exploited. Data & Society Research Institute.
[32] A Smith, and V Banic. 2016 Fake News: How a Partying Macedonian Teen Earns Thousands Publishing Lies. NBC News.
[33] PN Howard, B Ganesh, D Liotsiou, J Kelly, and C François. "The IRA and Political Polarization in the United States, 2012-2018." Computational Propaganda Research Project.
[34] A Arora, R Krishnan, A Nandkumar, R Telang, and Y Yang. 2004 Impact of Vulnerability Disclosure and Patch Availability-An Empirical Analysis. Third Workshop on the Economics of Information Security 24, 1268-1287.
[35] S Vegh. 2005 The Media's Portrayal of Hacking, Hackers, and Hacktivism Before and After September 11. First Monday, 10(2).
[36] T Ring. 2015 White Hats Versus Vendors: The Fight Goes On. Computer Fraud & Security, 2015(10), 12-17.
[37] V Jayaswal, W Yurcik, and D. Doss. 2002 Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?. IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology, 380-386.
[38] Society of Professional Journalists. 2014 Code of Ethics.
[39] K Barzilai-Nahon. 2008 Toward a Theory Of Network Gatekeeping: A Framework For Exploring Information Control. Journal of the American Society for Information Science and Technology, 59(9), 1493-1512.
[40] F Tripodi. 2018 Searching for Alternative Facts: Analyzing Scriptural Inference in Conservative News Practices. Data & Society Research Institute.
[41] R Caplan. 2018 Content or Context Moderation? Data & Society Research Institute.
[42] M Godwin. 1994 Meme, Counter-meme. Wired, 2(10), 10.
[43] M Vigil-Hayes, J Matthews, A Acker, and D Carter. 2018 Reflections on Alternative Internet Models and How They Inform More Mindful Connectivity. ITU Journal, ICT Discoveries, Special Issue 2, Data for Good.
[44] N Casemajor, S Couture, M Delfin, M Goerzen, and A Delfanti, 2015 Non-participation in Digital Media: Toward a Framework of Mediated Political Action. Media, Culture & Society, 37(6), 850-866.
[45] D Barney. 2014 Publics without Politics: Surplus Publicity as Depoliticization. In Publicity and the Canadian State, edited by K Kozolanka. University of Toronto Press, Toronto, Ontario, Canada.