The easy weaponization of social media: why profit has trumped security for U.S. companies

Sarah Oates

Published online: 11 May 2020
© Springer Nature Limited 2020

Abstract
American-based social media companies have become active players in digital war, both by accident of design and a subsequent failure to address the threat due to concerns over profits. Discussions about the negative role of social media in society generally address the myriad problems wrought by social media, including electoral manipulation, foreign disinformation, trolling, and deepfakes, as unfortunate side effects of a democratizing technology. This article argues that the design of social media fosters information warfare. With its current composition and lack of regulation, social media platforms such as Facebook and Twitter are active agents of disinformation, their destructive force in society outweighing their contributions to democracy. While this is not by deliberate design, the twin forces of capitalism and a lack of regulation of the world’s largest social media platforms have led to a situation in which social media are a key component of information war around the globe. This means that scholarly discussions should shift away from questions of ethics or actions (or lack thereof) on the part of social media companies to a frank focus on the security risk posed to democracy by social media.

Keywords Digital war · Social media · Facebook · Fifth dimension of war · Information war

This article departs from the usual discussion of the role of social media in society by comparing its value to its destructive elements. The problem with trying to “balance” both the benefits of social media such as its challenge to censorship and ability to aggregate social movements against destructive elements such as disinformation and the loss of privacy suggests we can somehow offset one side against the other. But if social media are making a country vulnerable to a key component of modern warfare, that really cannot be “balanced” even by the ability of social media to give voice to those often ignored by the mainstream media or to allow citizens to find affinity groups online. It’s like saying that we can find a “balance” for discussing other national security issues, such as the idea that while an enemy might have superior weapons, at least our nation spent more on social welfare over the past decade. It might be true, but it won’t help you win the war when the tanks roll over your borders.

As executives in Silicon Valley bristle at these ideas, let us first consider the nature of modern war and why information has become a key element of contemporary conflict. It is not so much that we need to understand the digital aspect of modern warfare; rather we need to see that digital warfare is a new way of understanding war in the digital age. Digital war is the central, rather than peripheral, issue. According to the Federation of American Scientists, digital war is “a subset of what we call information war, involves non-physical attacks on information, information processes, and information infrastructure that compromise, alter, damage, disrupt, or destroy information and/or delay, confuse, deceive, and disrupt information processing and decision making.” One of the most useful frames to consider information war is as the “fifth dimension” of warfare, joining land, sea, air, and space as spheres of battle (Franz 1996). Information war is more precise than the notion of “cyber war” (Hunker 2010). Indeed, the two concepts of “digital war” and “cyber war” are often conflated, given that “cyber” capabilities could be much broader than information operations and could embrace such tactics as dedicated denial of service (DDoS) attacks to bring down servers, the takeover of critical infrastructure via online or local malware, or even drone attacks that are programmed from afar.

---

Sarah Oates
soates@umd.edu

1 University of Maryland, College Park, USA

https://fas.org/irp/threat/cyber/docs/diw/ch4.html.
That kind of conflation is actually not useful, in that it reduces information to a subset of a broader phenomenon and underplays the critical role of information in conflict. While it is disruptive for a country to lose access to the internet due to an attack on a server, this does not have the same insidious danger as subversive propaganda. Cutting off access is an obvious act of war that has a clear solution. Infiltrating a media system, especially social media, in order to sow seeds of distrust in a way that undermines political institutions is a far more insidious and corrosive act of aggression against a society.

This discussion is focused on information war as it is carried out on social media, the battle for hearts and minds, as the most recent, critical development in modern warfare. Social media play a very important part in that war and social media are a critical part of both attack and defense in modern warfare. Indeed, information operations not only augment, but they often presage or even essentially replace conventional warfare. While the most publicized attack on democracy has been through attempted Russian influence in the U.S. elections, countries in Europe also have uncovered sustained anti-democracy campaigns by Russians in countries ranging from Estonia to the United Kingdom. While the U.S. and other countries are aware of the threats and are responding, this article argues that it is difficult to have a robust response when U.S. social media companies are key distribution nodes of foreign disinformation.

The ways in which narratives about coronavirus have become part of information warfare should sound a particularly ominous warning to democracies. A combination of fear, a large degree of unknown about the virus, as well as the rapid shifts in the evolution of the epidemic highlight how quickly disinformation can travel through social media at vulnerable moments. While national governments and major media outlets also are struggling with covering and framing the outbreak, social media platforms allow for authoritarian communication campaigns to widen and deepen the gaps between citizens and countries just when those connections are most desperately needed to combat an international health crisis. An example of this has been the attempt by authoritarian states (including China) to hint or even outright claim that the virus originated in a laboratory in the United States.

Now that it is impossible for social media companies to ignore the rising evidence of the central role of social media in inculcating conflict, they have defaulted to two key arguments in their defense: freedom of speech and the idea that the problem is limited to a fundamental misuse of their platforms. A core point emphasized by social media supporters was that the platforms were also vehicles for positive social change, such as in the Arab Spring, although the platforms showed very little ability or desire to adapt their programs to a range of national laws or norms. A 2008 article called “Doing Just Business or Just Doing Business” highlighted the problem: If internet companies choose to do business in China, for example, they must abide by China’s censorship rules. In the case of the Yahoo! email service, this meant turning over personal information on Hong Kong dissidents (Dann and Haddow 2008). Dann and Haddow argued that the companies had violated their ethical standards, in that it was reasonable to surmise that turning over the information would have adverse consequences for their users.

This ethical discussion, which took place before the current global reach of U.S. social media companies, now seems touchingly quaint. Dann and Haddow describe a world in which the main concerns were about privacy, censorship, and state surveillance, notably whether a country could compel an internet service provider to hand over personal information on its users. There was also disquiet about search engines being compliant with information filtering and collection regimes in non-free states. Social media companies still face these challenges, but they pale in the face of the ability of states to weaponize social media for both domestic and international use. In particular, the way that social media companies organize users into affinity groups (for example, by friending on Facebook or via hashtags on Twitter) makes it remarkably easy to find ways to manipulate these groups. When you add on the way that social media companies sell audiences to advertisers by identifying key markers via user activity (friends, posts, clicks, likes, shares, etc.), you have the ability to manipulate both domestic and foreign audiences as never before. While there has been outrage over Cambridge Analytica, the same capacity to identify and manipulate social media users still lies at the heart of the social media business model. And there is little sustained outrage over that.

Social media companies would (and do) argue that it’s unfair to blame the nature of social media itself if it winds up as the fifth dimension of warfare. Siva Vaidhyanathan disagrees: In his 2018 book Antisocial Media, Vaidhyanathan asserts that the entire design of social media makes it the perfect carrier for disinformation and that social media companies do little to counter this. Indeed, the arguments by Mark Zuckerberg and other social media officials are at best misinformed and, at worst, disingenuous. Given the evidence of the weaponization of social media and the particular lack of foreign citizens to have any right of redress against U.S. companies,2 it is clear that unregulated and mostly unresponsible dominant media platforms are choosing not to fundamentally change their business model.

Indeed, shareholders in Facebook, Twitter, and similar companies would not wish for greater policing of their

---

2 https://www.nytimes.com/2019/04/25/technology/facebook-regulation-ftc-fine.html.
platforms. The central element of the social media business model is the argument that social media companies are platforms, not providers, of information. This is protected by Section 230 of the U.S. Communication Decency Act, which states that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” This sounds a little circular but it means that the blame lies with the source of any problematic content, not the platform that provides the content. This has functioned as a get-out-of-jail-free card for Facebook and other internet providers if someone, for example, harasses or bullies or even threatens an individual or group. At the same time, Section 230 has been hailed by internet advocates as protection of free speech, which is true, but also (inadvertently) creates a great opportunity for proponents of disinformation.3

Section 230 is a very liberal interpretation of U.S. law, which is quite protective of free speech to the point that even hate speech is permissible in the United States. This has created some friction in the United States, but the truly dangerous aspect isn’t entirely domestic. It creates opportunities for digital war in two ways. First, it leaves the “digital borders” for disinformation more or less open for foreign states (this is aside from the problems of domestic disinformation). At the same time, as Facebook became the dominant social media platform around the world, citizens in other countries find themselves in the same dilemma. While citizens and their leaders discover they need to use the U.S.-based platform in order to communicate and even govern, at the same time social media platforms such as Facebook foster disinformation. They have introduced a communications system with a powerful virus of disinformation. This is exacerbated by the fact that Facebook also owns WhatsApp and Instagram, which carry the same problems. A U.S. freedom of speech model has set up a system through which disinformation flourishes and undermines democracy in countries worldwide.

It is not that social media companies are unaware or even naive about the way in which their platforms are used for disinformation. Rather, there are strong economic incentives for keeping the current laissez-faire ‘platform’ model. There are three key parts to the model: the needs of the advertisers are primary over those of the users; there is almost no vetting of the identity of who is posting; and content is virtually unmoderated. When content is moderated, it is automated as much as possible and this, so far, has been fairly ineffective.

---

3 Disinformation is the spreading of false information with the intention to deceive, for political or financial reasons.

---

Advertisers before all else

Ignoring the role of social media as the fifth dimension of war is lucrative, especially for Facebook. According to Facebook’s 2019 annual report,4 the company had revenue of $70.7 billion and earned $18.5 billion. Despite all the bad press about Facebook in the wake of the 2016 Russian election interference scandal, daily active users still increased by nine percent to 1.66 billion by the end of 2019. The number of employees at Facebook surged as well in 2019, with the company reporting 44,942 workers at the end of 2019, an increase of 26 percent in a single year. Overall, the company estimated that on average about 2.5 billion people used Facebook at least every month by end of 2019, an increase of eight percent in a single year. The company describes itself in the press release in this way: “Founded in 2004, Facebook’s mission is to give people the power to build community and bring the world closer together. People use Facebook’s apps and technologies to connect with friends and family, find communities and grow businesses.” The self-description highlights the deliberate self-deception: While Facebook does provide the services listed, it also furnishes an excellent way to spread malicious disinformation and propaganda to both domestic and foreign audiences.

If we want to return to the question of business ethics, one could argue that Facebook (and other social media companies) are continuing with a “hands off” business model to keep costs down and profits up. And it’s working. In the five years ended on December 31, 2019 (before the global financial shock from COVID-19), Facebook stock increased in value by about 163 percent, while the NASDAQ index was up about 87 percent over the same period.5 Allowing free access to the platform keeps revenue up and costs down.

This raises the question of whether social media could change so that there would be a better balance between the benefits and the drawbacks for society, notably the weaponization of social media to promote foreign disinformation. The real problem is that the users are not the financial priority of Facebook or almost any social media site. Rather, the advertisers are the key customers being served by the platform. In addition, the investors (in the form of shareholders) also rank far above the users in terms of company priorities. Almost any move made to protect the platform and its users from being used in digital war would adversely affect service to the advertisers and the shareholders.

---

4 https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx.

5 Figures calculated by the author.
Almost anyone can post

As the currency of social media platforms such as Facebook is in the number of users, you should keep barriers to entry as low as possible. Although Facebook is slightly harder to join than Twitter, it’s still relatively easy to create fake accounts. Changing a system in which artificial intelligence is overwhelmingly used to detect fake accounts would be expensive and cumbersome, but still possible (not least by having better AI). But there is a deeper problem. As the value of social media companies is based to a large degree on the number of users, it is not in the interest of the companies (or their shareholders) in either identifying fake accounts or in discouraging them in general. While social media companies may publicly condemn fake accounts and occasionally purge some, in reality fake accounts prop up their business model.

Lack of investment in moderation

Content moderation is a more complex issue for social media companies. On the one hand, better content moderation would make a more pleasant experience for a user seeking to avoid extreme speech, pornography, trolling, or what could be considered culturally inappropriate elements of the public sphere (or inappropriate for a particular age or group). Social media companies do moderate their content to screen out child pornography, extreme violence, etc., although even this is quite difficult. Yet, emotionally charged subject matter drives engagement (Celis et al. 2019). This dovetails with the need to attract consumers to the site so that they can be marketed to advertisers. Thus, a quiet, calm public sphere is not the best for their business model. It’s true that it would be much more expensive for social media companies to moderate either content or users in a more forceful and efficient way. But as with fake users, outrageous content also helps the bottom line. So it’s a lose–lose for social media companies to police their users and their content, as it would be far more costly and actually might reduce engagement. So their reluctance to do so is more than financial or logistical. Moderation works directly against their core economic interests as companies.

What is to be done?

If the economics of social media make it illogical for the platforms to change, how can we inculcate a shift in how social media works? If we stick to a dialogue that compares the benefits of social media to the problems of social media, we are unlikely to drive change. However, if citizens and policymakers alike are made aware of the critical role of U.S. social media companies in supporting information operations by foreign states, then change is more likely. This means making the central role of information warfare in modern conflict much more visible and compelling. This will take a significant shift in thinking for citizens, democratic leaders, and social media companies alike: In the American laissez-faire freedom of speech model, it is assumed that misinformation and even disinformation are just part of the marketplace of ideas. However, this is a misconception in a world in which information is deployed into highly engaged, yet highly segregated, communities of voters who are essentially walled off from fact-based journalism and information. In the United States, Russia and other foreign entities are able to deploy weapons of mass persuasion directly on vulnerable citizens, with both the vulnerabilities and the deployment system provided to a large degree by social media companies. This vulnerability also came into clearer view during the coronavirus epidemic, as propaganda released for financial and political gain added to the global ‘infodemic.’

In order to fully understand the role of social media companies in warfare, we need to return to the concept of the fifth dimension of war, i.e. information warfare. It is added to the first four dimensions of land, sea, air, and space. Information warfare is, of course, not a new phenomenon but it is radically changed and augmented by the digital sphere. In particular, the advent and wide adoption of social media around the globe gave a unique and unprecedented opportunity for countries to carry out information operations on the citizens of other states. The design of social media companies in warfare, we need to return to the concept of information operations by foreign states, then change is more likely. This means making the central role of information warfare in modern conflict much more visible and compelling. This will take a significant shift in thinking for citizens, democratic leaders, and social media companies alike: In the American laissez-faire freedom of speech model, it is assumed that misinformation and even disinformation are just part of the marketplace of ideas. However, this is a misconception in a world in which information is deployed into highly engaged, yet highly segregated, communities of voters who are essentially walled off from fact-based journalism and information. In the United States, Russia and other foreign entities are able to deploy weapons of mass persuasion directly on vulnerable citizens, with both the vulnerabilities and the deployment system provided to a large degree by social media companies. This vulnerability also came into clearer view during the coronavirus epidemic, as propaganda released for financial and political gain added to the global ‘infodemic.’

In other words, the design of social media companies is no longer an issue of pros and cons. According to analysts such as Vaidhyanathan, Facebook’s entire design creates the perfect operating theater for information warfare. With social media in its current state, this type of activity cannot be detected or curtailed in a reasonable way because it is embedded in the very nature of social media. It is so easy to pose as another, to gain trust, to polarize, and even convince people to change behavior that American corporations

---

6 https://247wallst.com/investing/2018/09/05/comparing-fake-account-detection-on-facebook-and-twitter/.

7 There is the counter-argument that a relatively pleasant and safe online sphere could be a significant attraction to users as well as provide significant political and social capital for social media companies. Any social capital, however, is far less valuable to the company than actual capital that is acquired through income streams and stock appreciation.
such as Facebook create a low-cost weapon for foreign enemies. Thus, American corporate ingenuity and business logic created a weapon that is deployed against Americans themselves.

This again brings up the problem of tradeoffs. Americans are now accustomed to the affordances of social media, including the idea that it is “free” to the user. In point of fact, user activity is harvested and sold to advertisers, so users are working for the social media companies in exchange for access. Few users, however, either realize or are particularly perturbed by that tradeoff. We could compare this to the rise of the automobile as a mode of transport. Initially, cars were seen as independent luxury items and there were few rules to govern their use. The early automobile age was accompanied by chaos and a high rate of accidents. Over time, governments took over regulation of the roads and—to a large degree—of car safety through the introduction of seat belts, anti-locking brakes, airbags, and other features. Yet, almost 40,000 Americans die in car accidents every year and tens of thousands more are injured. So Americans do accept trade-offs. But there has never been a national discussion about the security tradeoffs in social media. What is the level of safety that is necessary? How can we start a national conversation about this? Why is it a mistake to leave this in the hands of companies? How can we maintain a robust online sphere, but keep it much safer? Are citizens willing to pay for this, either directly or through government support?

Regulation

If the nature of the problem is framed as one of national security, can U.S. regulation work? Regulating social media is enormously difficult and that’s just in the United States, which has the advantage of being the headquarters of large Western social media companies. Much of this is due to excessive cyber-optimism in the United States, in particular as an echo of the origins of the internet as a research and educational tool outside of the commercial realm. Although that aspect of the internet has been long overshadowed by the commercial web, there is no comprehensive set of laws to specifically regulate the internet. Nor is there any public consensus on social media regulation, although just over half of Americans now believe that major tech companies should be more heavily regulated. But according to the Pew Research Center, Republicans feel that tech companies might already interfere with content too much: 85 percent of Republicans suspect that tech companies censor political viewpoints.

Can Americans be convinced that social media regulation is a security issue? We can turn to the issue of terrorism as a shift in thinking from civilian to defense issues. Prior to 9/11, the idea that U.S. citizens would go through body and luggage searches for all domestic flights would have been laughable. Yet, Americans and visitors now go through searches not only at airports, but in a wide range of other public spaces. While this is framed as a defense against foreign attacks, Americans face significant threats from domestic terrorism. Here is a silver lining to how illuminating the capabilities of social media as a tool for foreign actors to wage disinformation war against U.S. citizens is useful. American democracy also faces significant online domestic threats, from anti-vaxxers to hate groups to disinformation attacks on political opponents. Politically, though, there is no will to frame social media as a key part of that problem; rather, the general narrative is that disinformation is an unfortunate side effect of the social media we cannot live without.

To change this attitude on the part of Americans and U.S. social media companies, it will take a radical shift in understanding how social media has opened up a new and (so far) asymmetric battlefield for enemies of the American state. American perception of conflict and security shifted radically with 9/11. The threat of social media is much less visible and woven not only into the generally opaque nature of social media as people pose, pretend, and market themselves. It also comes at a time when the U.S. government is particularly weak as the political sphere is deeply split over the Trump administration’s actions.

That being said, Americans do seem to be waking up both to the threat and the lack of protection from social media companies. While Russian interference is seen through a strictly partisan lens, Chinese interference creates a much more unified response. Nor have social media executives won themselves much praise for their disingenuous performance at congressional hearings. As the coronavirus pandemic has led to heightened awareness of both the importance and vulnerability of trustworthy information, this could be a watershed moment in understanding and valuing the communication ecosystem. YouTube chief executive Susan Wojcicki said that the virus had been “an acceleration of our digital lives” and noted that it caused the platform to speed up changes to direct users to authoritative information. It is particularly relevant to consider how YouTube

---

8 https://carseurance.net/blog/car-accident-statistics/.
9 https://www.pewresearch.org/internet/2018/06/28/public-attitudes-toward-technology-companies/.
10 https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/04/20/the-technology-202-coronavirus-could-change-how-social-networks-approach-public-health/5e9cb4ec88e0fa101a7663d6/.
addressed health disinformation in the coronavirus pandemic, in that a study by the Oxford Internet Institute found that the platform had emerged as a “major purveyor of health and wellbeing information” (Marchal et al. 2020, p. 1). The Washington Post column that quoted Wojcicki speculated that health disinformation was taken more seriously than political disinformation by social media platforms.

The relative affordances of social media companies might baffle and confuse many Americans, but security threats never baffle or confuse Americans for long. All it will take is some relatively unified political leadership that can highlight this threat and Americans may indeed be ready for significant changes to the current social media model. Just as Americans pay a security tax for every airline flight, they may be willing to endorse a model of social media that is forced to take responsibility for its users and content. This will likely mean much more stringent government regulation and a change from Section 230. While this is disappointing for liberal concepts of free speech, free speech cannot work in a system in which it is weaponized by foreign adversaries.

References

Celis, L. Elisa, Sayash Kapoor, Farnood Salehi, and Nisheeth Vishnoi. 2019. Controlling Polarization in Personalization: An Algorithmic Framework. In The Proceedings of the Conference on Fairness, Accountability, and Transparency. New York: Association for Computing Machinery, 160–169.

Dann, G. Elijah, and Neil Haddow. 2008. Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! and the Business of Censoring China’s Internet. Journal of Business Ethics 79 (3): 219–234.

Franz, George J. 1996. Information—The Fifth Element of Combat Power. Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College.

Hunker, Jeffrey. 2010. Cyber War and Cyber Power: Issues for NATO Doctrine. Research Paper No. 62 (November). Rome: NATO Defense College.

Jamieson, Kathleen Hall. 2018. Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know. New York: Oxford University Press.

Marchal, Nahema, Hubert Au and Philip N. Howard. April 17, 2020. Coronavirus News and Information on YouTube: A Content Analysis of Popular Search Terms. COMPROP Data Memo 2020: 3 (COVID-19 Series). Oxford University: Oxford Internet Institute (OII).

Vaidhyanathan, Siva. 2018. Antisocial Media: How Facebook Disconnects Us and Undermines Democracy. New York: Oxford University Press.

Sarah Oates is Professor and Senior Scholar at the Philip Merrill College of Journalism, University of Maryland, College Park (USA). A former journalist, she has 25 years of experience in analyzing media production, content, and audiences. A major theme in her work is the way in which the traditional media and the internet can support or subvert democracy in places as diverse as Russia, the United States, and the United Kingdom.