MediaWell

News Item

The Next Big Internet Threat | POLITICO

By Joshua A. Geltzer & Dipayan Ghosh
October 30, 2018

> People are worried about what's happening on the internet—and they should be. In just the past few months, Americans have seen massive social turmoil over the deletion of conspiracy theorist Alex Jones' accounts from digital platforms; the public disclosure of criminal charges for Russian interference in the upcoming midterm elections; and other continuing developments in disinformation operations, such as the the Kremlin's new digital campaign to turn U.S. public opinion against taking military action against Bashar Assad's regime in Syria.
>
> But these latest incidents are only part of a far bigger trend. In our novel digital age, it has become far too easy for bad actors to spread harmful content far and wide, swiftly and with just the click of a button.
>
> All told, the internet age has seen four major waves of digital threats. None of these challenges has been entirely resolved, and the more recent of them remain serious threats, not just to the integrity of online dialogue but to American security and democracy. But the fifth wave is now fast upon us—and it might prove the thorniest of all.
>
> […]
>
> So, what will we see next in the social media universe? Thus far, we've witnessed four major waves of offensive content that have tracked the darkest tendencies in humanity—content that has exploited people (*sex*), spread vitriol (*hate*), encouraged ghastly attacks (*violence*) and duped electorates (*power*). Going forward, we fear a new kind of trend will emerge: "reputational exploitation," feeding off the human tendency to maximize self-interest while paying no heed to the rest of society—namely, through falsely disparagement of others for one's own benefit.

> Reputational exploitation would propagate various forms of content—and power the campaigns behind them—in an attempt to destroy, even temporarily, a competitor's reputation. This could take commercial form. Imagine a situation in which one investor wishes to spread negative information about a specific company so that she can artificially create and seize a forthcoming opportunity to short its stock. Or consider a company that wants to move public opinion against one of its rivals, so that it can attract some of the potential revenues at hand. (We've already seen the early manifestations of this through schemes to hack media outlets in efforts to obtain corporate press releases before they're released.)
>
> […]
>
> Tackling such future threats that might be even harder to discern than the ones we see today means shifting away from seeing each content policy challenge—child pornography, trolling, terrorist recruitment, election interference—as a distinct problem for the private sector and government to solve. Instead, the technology sector, informed and bolstered by government and civil society, must begin developing comprehensive approaches to ensuring that the internet doesn't become a place where nefarious activities—including disinformation operations—run rampant and gnaw at our proud democracy. Even as we fight rearguard actions to address the last waves of challenges, we must put in place the policies that can help us address the next ones—as well as mechanisms and channels that can be used to tackle content policy challenges in general, rather than having to engineer new solutions for every new type of challenge that crops up. Without such action and foresight, the very integrity of American democracy will be vulnerable to the agents of disinformation.

Source: The Next Big Internet Threat – POLITICO Magazine