MIT Technology Review

PHOTO OF PROTESTER WAVING EGYPT'S FLAG.

How social media took us from Tahrir Square to Donald Trump

To understand how digital technologies went from instruments for spreading democracy to weapons for attacking it, you have to look beyond the technologies themselves.

By Zeynep Tufekci August 14, 2018

1. The euphoria of discovery

As the Arab Spring convulsed the Middle East in 2011 and authoritarian leaders toppled one after another, I traveled the region to try to understand the role that technology was playing. I chatted with protesters in cafés near Tahrir Square in Cairo, and many asserted that as long as they had the internet and the smartphone, they would prevail. In Tunisia, emboldened activists showed me how they had used open-source tools to track the shopping trips to Paris that their autocratic president's wife had taken on government planes. Even Syrians I met in Beirut were still optimistic; their country had not yet descended into a hellish war. The young people had energy, smarts, humor, and smartphones, and we expected that the region's fate would turn in favor of their democratic demands.

Back in the United States, at a conference talk in 2012, I used a screenshot from a viral video recorded during the Iranian street protests of 2009 to illustrate how the new technologies were making it harder for traditional information gatekeepers—like governments and the media—to stifle or control dissident speech. It was a difficult image to see: a young woman lay bleeding to death on the sidewalk. But therein resided its power. Just a decade earlier, it would most likely never have been taken (who carried video cameras all the time?), let alone gone viral (how, unless you owned a TV station or a newspaper?). Even if a news photographer had happened to be there, most news organizations wouldn't have shown such a graphic image.

At that conference, I talked about the role of social media in breaking down what social scientists call "pluralistic ignorance"—the belief that one is alone in one's views when in

reality everyone has been collectively silenced. That, I said, was why social media had fomented so much rebellion: people who were previously isolated in their dissent found and drew strength from one another.

Digital connectivity provided the spark, but the kindling was everywhere.
Peter Macdiarmid | Getty Images

Twitter, the company, retweeted my talk in a call for job applicants to "join the flock." The implicit understanding was that Twitter was a force for good in the world, on the side of the people and their revolutions. The new information gatekeepers, which didn't see themselves as gatekeepers but merely as neutral "platforms," nonetheless liked the upending potential of their technologies.

I shared in the optimism. I myself hailed from the Middle East and had been watching dissidents use digital tools to challenge government after government.

But a shift was already in the air.

During the Tahrir uprising, Egypt's weary autocrat, Hosni Mubarak, had clumsily cut off internet and cellular service. The move backfired: it restricted the flow of information

coming out of Tahrir Square but caused international attention on Egypt to spike. He hadn't understood that in the 21st century it is the flow of attention, not information (which we already have too much of), that matters. Besides, friends of the spunky Cairo revolutionaries promptly flew in with satellite phones, allowing them to continue giving interviews and sending images to global news organizations that now had even more interest in them.

Within a few weeks, Mubarak was forced out. A military council replaced him. What it did then foreshadowed much of what was to come. Egypt's Supreme Council of the Armed Forces promptly opened a Facebook page and made it the exclusive outlet for its communiqués. It had learned from Mubarak's mistakes; it would play ball on the dissidents' turf.

The generals in Egypt learned from Hosni Mubarak's mistakes.
Peter Macdiarmid/Getty Images

Within a few years, Egypt's online sphere would change dramatically. "We had more influence when it was just us on Twitter," one activist prominent on social media told me. "Now it is full of bickering between dissidents [who are] being harassed by

government supporters." In 2013, on the heels of protests against a fledgling but divisive civilian government, the military would seize control.

Power always learns, and powerful tools always fall into its hands. This is a hard lesson of history but a solid one. It is key to understanding how, in seven years, digital technologies have gone from being hailed as tools of freedom and change to being blamed for upheavals in Western democracies—for enabling increased polarization, rising authoritarianism, and meddling in national elections by Russia and others.

But to fully understand what has happened, we also need to examine how human social dynamics, ubiquitous digital connectivity, and the business models of tech giants combine to create an environment where misinformation thrives and even true information can confuse and paralyze rather than informing and illuminating.

2. The audacity of hope

Barack Obama's election in 2008 as the first African-American president of the United States had prefigured the Arab Spring's narrative of technology empowering the underdog. He was an unlikely candidate who had emerged triumphant, beating first Hillary Clinton in the Democratic primary and then his Republican opponent in the general election. Both his 2008 and 2012 victories prompted floods of laudatory articles on his campaign's tech-savvy, data-heavy use of social media, voter profiling, and microtargeting. After his second win, *MIT Technology Review* featured Bono on its cover, with the headline "Big Data Will Save Politics" and a quote: "The mobile phone, the Net, and the spread of information—a deadly combination for dictators."

However, I and many others who watched authoritarian regimes were already worried. A key issue for me was how microtargeting, especially on Facebook, could be used to wreak havoc with the public sphere. It was true that social media let dissidents know they were not alone, but online microtargeting could also create a world in which you wouldn't know what messages your neighbors were getting or how the ones aimed at you were being tailored to your desires and vulnerabilities.

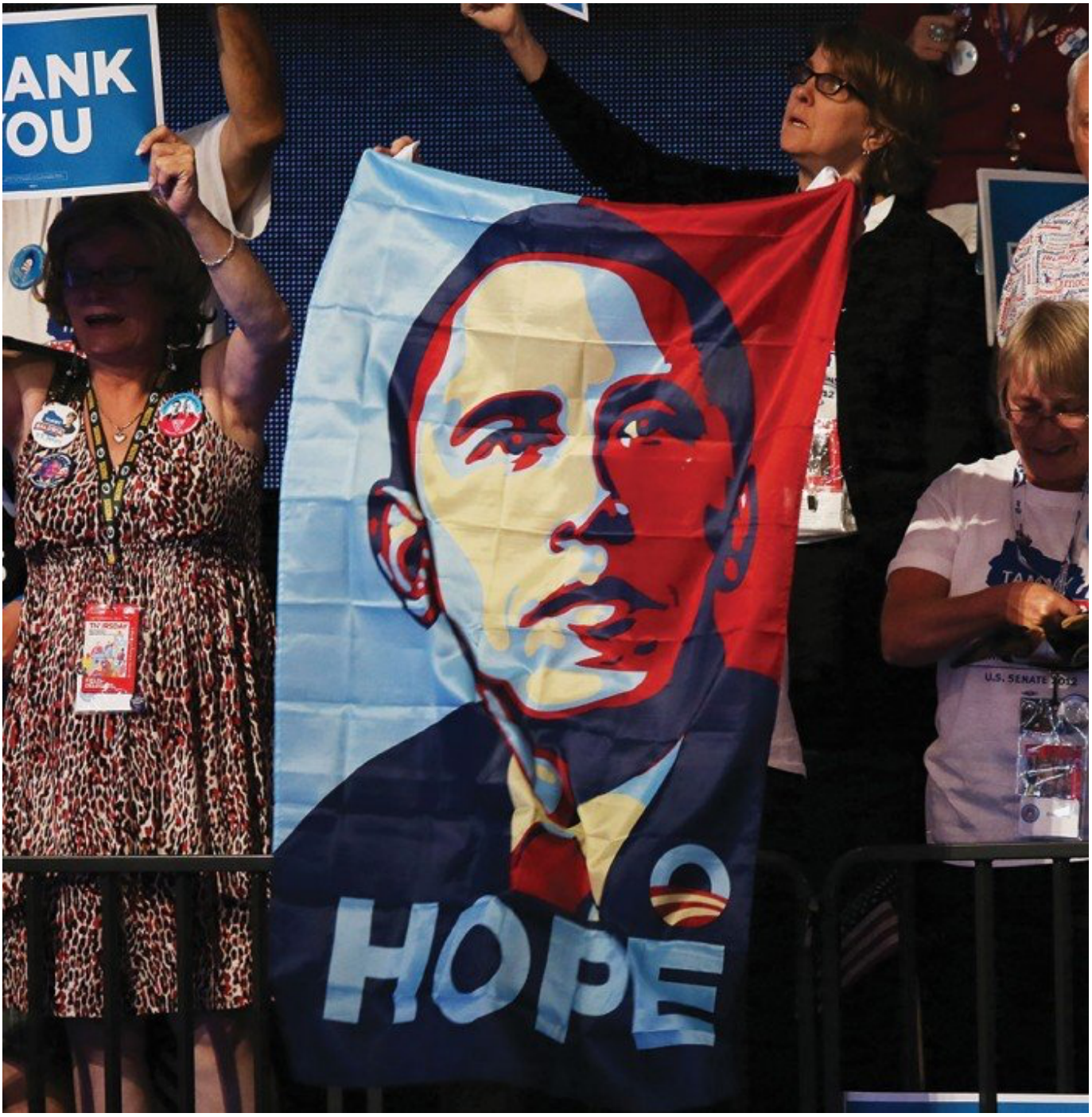
Digital platforms allowed communities to gather and form in new ways, but they also dispersed existing communities, those that had watched the same TV news and read the same newspapers. Even living on the same street meant less when information

was disseminated through algorithms designed to maximize revenue by keeping people glued to screens. It was a shift from a public, collective politics to a more private, scattered one, with political actors collecting more and more personal data to figure out how to push just the right buttons, person by person and out of sight.

All this, I feared, could be a recipe for misinformation and polarization.

Shortly after the 2012 election, I wrote an op-ed for the *New York Times* voicing these worries. Not wanting to sound like a curmudgeon, I understated my fears. I merely advocated transparency and accountability for political ads and content on social media, similar to systems in place for regulated mediums like TV and radio.

The backlash was swift. Ethan Roeder, the data director for the Obama 2012 campaign, wrote a piece headlined "I Am Not Big Brother," calling such worries "malarkey." Almost all the data scientists and Democrats I talked to were terribly irritated by my idea that technology could be anything but positive. Readers who commented on my op-ed thought I was just being a spoilsport. Here was a technology that allowed Democrats to be better at elections. How could this be a problem?



There were laudatory articles about Barack Obama's use of voter profiling and microtargeting.
Alex wong/getty Images

3. The illusion of immunity

The Tahrir revolutionaries and the supporters of the US Democratic Party weren't alone in thinking they would always have the upper hand.

The US National Security Agency had an arsenal of hacking tools based on vulnerabilities in digital technologies—bugs, secret backdoors, exploits, shortcuts in the (very advanced) math, and massive computing power. These tools were dubbed "nobody but us" (or NOBUS, in the acronym-loving intelligence community), meaning

no one else could exploit them, so there was no need to patch the vulnerabilities or make computer security stronger in general. The NSA seemed to believe that weak security online hurt its adversaries a lot more than it hurt the NSA.

That confidence didn't seem unjustified to many. After all, the internet is mostly an American creation; its biggest companies were founded in the United States. Computer scientists from around the world still flock to the country, hoping to work for Silicon Valley. And the NSA has a giant budget and, reportedly, thousands of the world's best hackers and mathematicians.

Since it's all classified, we cannot know the full story, but between 2012 and 2016 there was at least no readily visible effort to significantly "harden" the digital infrastructure of the US. Nor were loud alarms raised about what a technology that crossed borders might mean. Global information flows facilitated by global platforms meant that someone could now sit in an office in Macedonia or in the suburbs of Moscow or St. Petersburg and, for instance, build what appeared to be a local news outlet in Detroit or Pittsburgh.

There doesn't seem to have been a major realization within the US's institutions—its intelligence agencies, its bureaucracy, its electoral machinery—that true digital security required both better technical infrastructure and better public awareness about the risks of hacking, meddling, misinformation, and more. The US's corporate dominance and its technical wizardry in some areas seemed to have blinded the country to the brewing weaknesses in other, more consequential ones.

4. The power of the platforms

In that context, the handful of giant US social-media platforms seem to have been left to deal as they saw fit with what problems might emerge. Unsurprisingly, they prioritized their stock prices and profitability. Throughout the years of the Obama administration, these platforms grew boisterously and were essentially unregulated. They spent their time solidifying their technical chops for deeply surveilling their users, so as to make advertising on the platforms ever more efficacious. In less than a decade, Google and Facebook became a virtual duopoly in the digital ad market.

Facebook also gobbled up would-be competitors like WhatsApp and Instagram

without tripping antitrust alarms. All this gave it more data, helping it improve its algorithms for keeping users on the platform and targeting them with ads. Upload a list of already identified targets and Facebook's AI engine will helpfully find much bigger "look-alike" audiences that may be receptive to a given message. After 2016, the grave harm this feature could do would become obvious.

Meanwhile, Google—whose search rankings can make or break a company, service, or politician, and whose e-mail service had a billion users by 2016—also operated the video platform YouTube, increasingly a channel for information and propaganda around the world. A *Wall Street Journal* investigation earlier this year found that YouTube's recommendation algorithm tended to drive viewers toward extremist content by suggesting edgier versions of whatever they were watching—a good way to hold their attention.

This was lucrative for YouTube but also a boon for conspiracy theorists, since people are drawn to novel and shocking claims. "Three degrees of Alex Jones" became a running joke: no matter where you started on YouTube, it was said, you were never more than three recommendations away from a video by the right-wing conspiracist who popularized the idea that the Sandy Hook school shooting in 2012 had never happened and the bereaved parents were mere actors playing parts in a murky conspiracy against gun owners.

Though smaller than Facebook and Google, Twitter played an outsize role thanks to its popularity among journalists and politically engaged people. Its open philosophy and easygoing approach to pseudonyms suits rebels around the world, but it also appeals to anonymous trolls who hurl abuse at women, dissidents, and minorities. Only earlier this year did it crack down on the use of bot accounts that trolls used to automate and amplify abusive tweeting.

Twitter's pithy, rapid-fire format also suits anyone with a professional or instinctual understanding of attention, the crucial resource of the digital economy.

Say, someone like a reality TV star. Someone with an uncanny ability to come up with belittling, viral nicknames for his opponents, and to make boastful promises that resonated with a realignment in American politics—a realignment mostly missed by

both Republican and Democratic power brokers.

Donald Trump's campaign excelled at using Facebook as it was designed to be used by advertisers.
Brett Carlsen/Stringer/Getty Images

Donald Trump, as is widely acknowledged, excels at using Twitter to capture attention. But his campaign also excelled at using Facebook as it was designed to be used by advertisers, testing messages on hundreds of thousands of people and microtargeting them with the ones that worked best. Facebook had embedded its own employees within the Trump campaign to help it use the platform effectively (and thus spend a lot of money on it), but they were also impressed by how well Trump himself performed. In later internal memos, reportedly, Facebook would dub the Trump campaign an "innovator" that it might learn from. Facebook also offered its services to Hillary Clinton's campaign, but it chose to use them much less than Trump's did.

Digital tools have figured significantly in political upheavals around the world in the past few years, including others that left elites stunned: Britain's vote to leave the European Union, and the far right's gains in Germany, Hungary, Sweden, Poland, France, and elsewhere. Facebook helped Philippine strongman Rodrigo Duterte with his election strategy and was even cited in a UN report as having contributed to the ethnic-

cleansing campaign against the Rohingya minority in Myanmar.

However, social media isn't the only seemingly democratizing technology that extremists and authoritarians have co-opted. Russian operatives looking to hack into the communications of Democratic Party officials used Bitcoin—a cryptocurrency founded to give people anonymity and freedom from reliance on financial institutions—to buy tools such as virtual private networks, which can help one cover one's traces online. They then used these tools to set up fake local news organizations on social media across the US.

There they started posting materials aimed at fomenting polarization. The Russian trolls posed as American Muslims with terrorist sympathies and as white supremacists who opposed immigration. They posed as Black Lives Matter activists exposing police brutality and as people who wanted to acquire guns to shoot police officers. In so doing, they not only fanned the flames of division but provided those in each group with evidence that their imagined opponents were indeed as horrible as they suspected. These trolls also incessantly harassed journalists and Clinton supporters online, resulting in a flurry of news stories about the topic and fueling a (self-fulfilling) narrative of polarization among the Democrats.

5. The lessons of the era

How did all this happen? How did digital technologies go from empowering citizens and toppling dictators to being used as tools of oppression and discord? There are several key lessons.

The NSA had an arsenal of hacking tools dubbed NOBUS.

First, the weakening of old-style information gatekeepers (such as media, NGOs, and government and academic institutions), while empowering the underdogs, has also, in another way, deeply disempowered underdogs. Dissidents can more easily circumvent censorship, but the public sphere they can now reach is often too noisy and confusing for them to have an impact. Those hoping to make positive social change have to convince people both that something in

the world needs changing and there is a constructive, reasonable way to change it. Authoritarians and extremists, on the other hand, often merely have to muddy the waters and weaken trust in general so that everyone is too fractured and paralyzed to act. The old gatekeepers blocked some truth and dissent, but they blocked many forms of misinformation too.

The old information gatekeepers blocked some truth and dissent but also many forms of misinformation.
Chip Somodevilla/Getty Images

Second, the new, algorithmic gatekeepers aren't merely (as they like to believe) neutral conduits for both truth and falsehood. They make their money by keeping people on their sites and apps; that aligns their incentives closely with those who stoke outrage, spread misinformation, and appeal to people's existing biases and preferences. Old gatekeepers failed in many ways, and no doubt that failure helped fuel mistrust and doubt; but the new gatekeepers *succeed* by fueling mistrust and doubt, as long as the clicks keep coming.

Third, the loss of gatekeepers has been especially severe in local journalism. While some big US media outlets have managed (so far) to survive the upheaval wrought by the internet, this upending has almost completely broken local newspapers, and it has

hurt the industry in many other countries. That has opened fertile ground for misinformation. It has also meant less investigation of and accountability for those who exercise power, especially at the local level. The Russian operatives who created fake local media brands across the US either understood the hunger for local news or just lucked into this strategy. Without local checks and balances, local corruption grows and trickles up to feed a global corruption wave playing a major part in many of the current political crises.

The fourth lesson has to do with the much-touted issue of filter bubbles or echo chambers—the claim that online, we encounter only views similar to our own. This isn't completely true. While algorithms will often feed people some of what they already want to hear, research shows that we probably encounter a wider variety of opinions online than we do offline, or than we did before the advent of digital tools.

Rather, the problem is that when we encounter opposing views in the age and context of social media, it's not like reading them in a newspaper while sitting alone. It's like hearing them from the opposing team while sitting with our fellow fans in a football stadium. Online, we're connected with our communities, and we seek approval from our like-minded peers. We bond with our team by yelling at the fans of the other one. In sociology terms, we strengthen our feeling of "in-group" belonging by increasing our distance from and tension with the "out-group"—us versus them. Our cognitive universe isn't an echo chamber, but our social one is. This is why the various projects for fact-checking claims in the news, while valuable, don't convince people. Belonging is stronger than facts.

A similar dynamic played a role in the aftermath of the Arab Spring. The revolutionaries were caught up in infighting on social media as they broke into ever smaller groups, while at the same time authoritarians were mobilizing their own supporters to attack the dissidents, defining them as traitors or foreigners. Such "patriotic" trolling and harassment is probably more common, and a bigger threat to dissidents, than attacks orchestrated by governments.

This is also how Russian operatives fueled polarization in the United States, posing simultaneously as immigrants and white supremacists, angry Trump supporters and "Bernie bros." The content of the argument didn't matter; they were looking to paralyze

and polarize rather than convince. Without old-style gatekeepers in the way, their messages could reach anyone, and with digital analytics at their fingertips, they could hone those messages just like any advertiser or political campaign.

Fifth, and finally, Russia exploited the US's weak digital security—its "nobody but us" mind-set—to subvert the public debate around the 2016 election. The hacking and release of e-mails from the Democratic National Committee and the account of Clinton campaign manager John Podesta amounted to a censorship campaign, flooding conventional media channels with mostly irrelevant content. As the Clinton e-mail scandal dominated the news cycle, neither Trump's nor Clinton's campaign got the kind of media scrutiny it deserved.

This shows, ultimately, that "nobody but us" depended on a mistaken interpretation of what digital security means. The US may well still have the deepest offensive capabilities in cybersecurity. But Podesta fell for a phishing e-mail, the simplest form of hacking, and the US media fell for attention hacking. Through their hunger for clicks and eyeballs, and their failure to understand how the new digital sphere operates, they were diverted from their core job into a confusing swamp. Security isn't just about who has more Cray supercomputers and cryptography experts but about understanding how attention, information overload, and social bonding work in the digital era.

There are no easy answers, and no purely digital answers.

This potent combination explains why, since the Arab Spring, authoritarianism and misinformation have thrived, and a free-flowing contest of ideas has not. Perhaps the simplest statement of the problem, though, is encapsulated in Facebook's original mission statement (which the social network changed in 2017, after a backlash against its role in spreading misinformation). It was to make the world "more open and connected." It turns out that this isn't necessarily an unalloyed good. Open to *what*, and connected *how*? The need to ask those questions is perhaps the biggest lesson of all.

6. The way forward

What is to be done? There are no easy answers. More important, there are no purely digital answers.

There are certainly steps to be taken in the digital realm. The weak antitrust environment that allowed a few giant companies to become near-monopolies should be reversed. However, merely breaking up these giants without changing the rules of the game online may simply produce a lot of smaller companies that use the same predatory techniques of data surveillance, microtargeting, and "nudging."

Ubiquitous digital surveillance should simply end in its current form. There is no justifiable reason to allow so many companies to accumulate so much data on so many people. Inviting users to "click here to agree" to vague, hard-to-pin-down terms of use doesn't produce "informed consent." If, two or three decades ago, before we sleepwalked into this world, a corporation had suggested so much reckless data collection as a business model, we would have been horrified.

There are many ways to operate digital services without siphoning up so much personal data. Advertisers have lived without it before, they can do so again, and it's probably better if politicians can't do it so easily. Ads can be attached to content, rather than directed to people: it's fine to advertise scuba gear to me if I am on a divers' discussion board, for example, rather than using my behavior on other sites to figure out that I'm a diver and then following me around everywhere I go—online or offline.

But we didn't get where we are simply because of digital technologies. The Russian government may have used online platforms to remotely meddle in US elections, but Russia did not create the conditions of social distrust, weak institutions, and detached elites that made the US vulnerable to that kind of meddling.

Russia meddled in US politics, but it didn't create the conditions that made the US vulnerable to such meddling.
Chris McGrath/Getty Images

Russia did not make the US (and its allies) initiate and then terribly mishandle a major war in the Middle East, the after-effects of which—among them the current refugee crisis—are still wreaking havoc, and for which practically nobody has been held responsible. Russia did not create the 2008 financial collapse: that happened through corrupt practices that greatly enriched financial institutions, after which all the culpable parties walked away unscathed, often even richer, while millions of Americans lost their jobs and were unable to replace them with equally good ones.

Russia did not instigate the moves that have reduced Americans' trust in health authorities, environmental agencies, and other regulators. Russia did not create the revolving door between Congress and the lobbying firms that employ ex-politicians at handsome salaries. Russia did not defund higher education in the United States. Russia did not create the global network of tax havens in which big corporations and the rich can pile up enormous wealth while basic government services get cut.

These are the fault lines along which a few memes can play an outsize role. And not just Russian memes: whatever Russia may have done, domestic actors in the United

States and Western Europe have been eager, and much bigger, participants in using digital platforms to spread viral misinformation.

Even the free-for-all environment in which these digital platforms have operated for so long can be seen as a symptom of the broader problem, a world in which the powerful have few restraints on their actions while everyone else gets squeezed. Real wages in the US and Europe are stuck and have been for decades while corporate profits have stayed high and taxes on the rich have fallen. Young people juggle multiple, often mediocre jobs, yet find it increasingly hard to take the traditional wealth-building step of buying their own home—unless they already come from privilege and inherit large sums.

If digital connectivity provided the spark, it ignited because the kindling was already everywhere. The way forward is not to cultivate nostalgia for the old-world information gatekeepers or for the idealism of the Arab Spring. It's to figure out how our institutions, our checks and balances, and our societal safeguards should function in the 21st century—not just for digital technologies but for politics and the economy in general. This responsibility isn't on Russia, or solely on Facebook or Google or Twitter. It's on us.

*Zeynep Tufekci is an associate professor at the University of North Carolina and a contributing opinion writer at the*New York Times.
