Adam Maida

A Guide to Understanding the Hoax of the Century

Thirteen ways of looking at disinformation

By Jacob Siegel

March 28, 2023

Prologue: The Information War

In 1950, Sen. Joseph McCarthy claimed that he had proof of a communist spy ring operating inside the government. Overnight, the explosive accusations blew up in the national press, but the details kept changing. Initially, McCarthy said he had a list with the names of 205 communists in the State Department; the next day he revised it to 57. Since he kept the list a secret, the inconsistencies were beside the point. The point was the power of the accusation, which made McCarthy's name synonymous with the politics of the era.

For more than half a century, McCarthyism stood as a defining chapter in the worldview of American liberals: a warning about the dangerous allure of blacklists, witch hunts, and demagogues.

Until 2017, that is, when another list of alleged Russian agents roiled the American press and political class. A new outfit called Hamilton 68 claimed to have discovered hundreds of Russian-affiliated accounts that had infiltrated Twitter to sow chaos and help Donald Trump win the election. Russia stood accused of hacking social media platforms, the new centers of power, and using them to covertly direct events inside the United States.

None of it was true. After reviewing Hamilton 68's secret list, Twitter's safety officer, Yoel Roth, privately admitted that his company was allowing "real people" to be "unilaterally labeled Russian stooges without evidence or recourse."

The Hamilton 68 episode played out as a nearly shot-for-shot remake of the McCarthy affair, with one important difference: McCarthy faced some resistance from leading journalists as well as from the U.S. intelligence agencies and his fellow members of Congress. In our time, those same groups lined up to support the new secret lists and attack anyone who questioned them.

When proof emerged earlier this year that Hamilton 68 was a high-level hoax perpetrated against the American people, it was met with a great wall of silence in the national press. The disinterest was so profound, it suggested a matter of principle rather than convenience for the standard-bearers of American liberalism who had lost faith in the promise of freedom and embraced a new ideal.

In his last days in office, President Barack Obama made the decision to set the country on a new course. On Dec. 23, 2016, he signed into law the Countering Foreign Propaganda and Disinformation Act, which used the language of defending the homeland to launch an open-ended, offensive information war.

Something in the looming specter of Donald Trump and the populist movements of 2016 reawakened sleeping monsters in the West. Disinformation, a half-forgotten relic of the Cold War, was newly spoken of as an urgent, existential threat. Russia was said to have exploited the vulnerabilities of the open internet to bypass U.S. strategic defenses by infiltrating private citizens' phones and laptops. The Kremlin's endgame was to colonize the minds of its targets, a tactic cyber warfare specialists call "cognitive hacking."

Defeating this specter was treated as a matter of national survival. "The U.S. Is Losing at Influence Warfare," warned a December 2016 article in the defense industry journal, Defense One. The article quoted two government insiders arguing that laws written to protect U.S. citizens from state spying were jeopardizing national security. According to Rand Waltzman, a former program manager at the Defense Advanced Research Projects Agency, America's adversaries enjoyed a "significant advantage" as the result of "legal and organizational constraints that we are subject to and they are not."

The point was echoed by Michael Lumpkin, who headed the State Department's Global Engagement Center (GEC), the agency Obama designated to run the U.S. counter-disinformation campaign. Lumpkin singled out the Privacy Act of 1974, a post-Watergate law protecting U.S. citizens from having their data collected by the government, as antiquated. "The 1974 act was created to make sure that we aren't collecting data on U.S. citizens. Well, … by definition the World Wide Web is worldwide. There is no passport that goes with it. If it's a Tunisian citizen in the United States or a U.S. citizen in Tunisia, I don't have the ability to discern that … If I had more ability to work with that [personally identifiable information] and had access … I could do more targeting, more definitively, to make sure I could hit the right message to the right audience at the right time."

The message from the U.S. defense establishment was clear: To win the information war—an existential conflict taking place in the borderless dimensions of cyberspace—the government needed to dispense with outdated legal distinctions between foreign terrorists and American citizens.

Since 2016, the federal government has spent billions of dollars on turning the counter-disinformation complex into one of the most powerful forces in the modern world: a sprawling leviathan with tentacles reaching into both the public and private sector, which the government uses to direct a "whole of society" effort that aims to seize total control over the internet and achieve nothing less than the eradication of human error.

Step one in the national mobilization to defeat disinfo fused the U.S. national security infrastructure with the social media platforms, where the war was being fought. The government's lead counter-disinformation agency, the GEC, declared that its mission entailed "seeking out and engaging the best talent within the technology sector." To that end, the government started deputizing tech executives as de facto wartime information commissars.

At companies like Facebook, Twitter, Google, and Amazon, the upper management levels had always included veterans of the national security establishment. But with the new alliance between U.S. national security and social media, the former spooks and intelligence agency officials grew into a dominant bloc inside those companies; what had been a career ladder by which people stepped up from their government experience to reach private tech-sector jobs turned into an ouroboros that molded the two together. With the D.C.-Silicon Valley fusion, the federal bureaucracies could rely on informal social connections to push their agenda inside the tech companies.

In the fall of 2017, the FBI opened its Foreign Influence Task Force for the express purpose of monitoring social media to flag accounts trying to "discredit U.S. individuals and institutions." The Department of Homeland Security took on a similar role.

At around the same time, Hamilton 68 blew up. Publicly, Twitter's algorithms turned the Russian-influence-exposing "dashboard" into a major news story. Behind the scenes, Twitter executives quickly figured out that it was a scam. When Twitter reverse-engineered the secret list, it found, according to the journalist Matt Taibbi, that "instead of tracking how Russia influenced American attitudes, Hamilton 68 simply collected a handful of mostly real, mostly American accounts and described their organic conversations as Russian scheming." The discovery prompted Twitter's head of trust and safety, Yoel Roth, to suggest in an October 2017 email that the company take action to expose the hoax and "call this out on the bullshit it is."

In the end, neither Roth nor anyone else said a word. Instead, they let a purveyor of industrial-grade bullshit—the old-fashioned term for *disinformation*—continue dumping its contents directly into the news stream.

It was not enough for a few powerful agencies to combat disinformation. The strategy of national mobilization called for "not only the whole-of-government, but also whole-of-society" approach, according to a document released by the GEC in 2018. "To counter propaganda and disinformation," the agency stated, "will require leveraging expertise from across government, tech and marketing sectors, academia, and NGOs."

This is how the government-created "war against disinformation" became the great moral crusade of its time. CIA officers at Langley came to share a cause with hip young journalists in Brooklyn, progressive nonprofits in D.C., George Soros-funded think tanks in Prague, racial equity consultants, private equity consultants, tech company staffers in Silicon Valley, Ivy League researchers, and failed British royals. Never Trump Republicans joined forces with the Democratic National Committee, which declared online disinformation "a whole-of-society problem that requires a whole-of-society response."

Even trenchant critics of the phenomenon—including Taibbi and the *Columbia Journalism Review*'s Jeff Gerth, who recently published a dissection of the press's role in promoting false Trump-Russia collusion claims—have focused on the media's failures, a framing largely shared by conservative publications, which treat disinformation as an issue of partisan censorship bias. But while there's no question that the media has utterly disgraced itself, it's also a convenient fall guy—by far the weakest player in the counter-disinformation complex. The American press, once the guardian of democracy, was hollowed out to the point that it could be worn like a hand puppet by the U.S. security agencies and party operatives.

It would be nice to call what has taken place a tragedy, but an audience is meant to learn something from a tragedy. As a nation, America not only has learned nothing, it has been deliberately prevented from learning anything while being made to chase after shadows. This is not because Americans are stupid; it's because what has taken place is not a tragedy but something closer to a crime. Disinformation is both the name of the crime and the means of covering it up; a weapon that doubles as a disguise.

The crime is the information war itself, which was launched under false pretenses and by its nature destroys the essential boundaries between the public and private and between the foreign and domestic, on which peace and democracy depend. By conflating the anti-establishment politics of domestic populists with acts of war by foreign enemies, it justified turning weapons of war against Americans citizens. It turned the public arenas where social and political life take

place into surveillance traps and targets for mass psychological operations. The crime is the routine violation of Americans' rights by unelected officials who secretly control what individuals can think and say.

What we are seeing now, in the revelations exposing the inner workings of the state-corporate censorship regime, is only the end of the beginning. The United States is still in the earliest stages of a mass mobilization that aims to harness every sector of society under a singular technocratic rule. The mobilization, which began as a response to the supposedly urgent menace of Russian interference, now evolves into a regime of total information control that has arrogated to itself the mission of eradicating abstract dangers such as error, injustice, and harm—a goal worthy only of leaders who believe themselves to be infallible, or comic-book supervillains.

The first phase of the information war was marked by distinctively human displays of incompetence and brute-force intimidation. But the next stage, already underway, is being carried out through both scalable processes of artificial intelligence and algorithmic pre-censorship that are invisibly encoded into the infrastructure of the internet, where they can alter the perceptions of billions of people.

Something monstrous is taking shape in America. Formally, it exhibits the synergy of state and corporate power in service of a tribal zeal that is the hallmark of fascism. Yet anyone who spends time in America and is not a brainwashed zealot can tell that it is not a fascist country. What is coming into being is a new form of government and social organization that is as different from mid-twentieth century liberal democracy as the early American republic was from the British monarchism that it grew out of and eventually supplanted. A state organized on the principle that it exists to protect the sovereign rights of individuals, is being replaced by a digital leviathan that wields power through opaque algorithms and the manipulation of digital swarms. It resembles the Chinese system of social credit and one-party state control, and yet that, too, misses the distinctively American and providential character of the control system. In the time we lose trying to name it, the thing itself may disappear back into the bureaucratic shadows, covering up any trace of it with automated deletions from the top-secret data centers of Amazon Web Services, "the trusted cloud for government."

> When the blackbird flew out of sight,
> It marked the edge
> Of one of many circles.

In a technical or structural sense, the censorship regime's aim is not to censor or to oppress, but to rule. That's why the authorities can never be labeled as guilty of disinformation. Not when they lied about Hunter Biden's laptops, not when they claimed that the lab leak was a racist conspiracy, not when they said that vaccines stopped transmission of the novel coronavirus. Disinformation, now and for all time, is whatever they say it is. That is not a sign that the concept is being misused or corrupted; it is the precise functioning of a totalitarian system.

If the underlying philosophy of the war against disinformation can be expressed in a single claim, it is this: You cannot be trusted with your own mind. What follows is an attempt to see how this philosophy has manifested in reality. It approaches the subject of disinformation from 13 angles—like the "Thirteen Ways of Looking at a Blackbird," Wallace Stevens' 1917 poem—with the aim that the composite of these partial views will provide a useful impression of disinformation's true shape and ultimate design.

CONTENTS

Have insider information on the counter-disinformation complex? Email jacobsiegel@protonmail.com or contact him or contact him on Twitter @jacob__siegel.

I. Russophobia Returns, Unexpectedly: The Origins of Contemporary “Disinformation”

The foundations of the current information war were laid in response to a sequence of events that took place in 2014. First Russia tried to suppress the U.S.-backed Euromaidan movement in Ukraine; a few months later Russia invaded Crimea; and several months after that the Islamic State captured the city of Mosul in northern Iraq and declared it the capital of a new caliphate. In three separate conflicts, an enemy or rival power of the United States was seen to have successfully used not just military might but also social media messaging campaigns designed to confuse and demoralize its enemies—a combination known as “hybrid warfare.” These conflicts convinced U.S. and NATO security officials that the power of social media to shape public perceptions had evolved to the point where it could decide the outcome of modern wars—outcomes that might be counter to those the United States wanted. They concluded that the state had to acquire the means to take control over digital communications so that they could present reality as they wanted it to be, and prevent reality from becoming anything else.

Technically, *hybrid warfare* refers to an approach that combines military and non-military means—overt and covert operations mixed with cyberwarfare and influence operations—to both confuse and weaken a target while avoiding direct, full-scale conventional war. In practice, it is notoriously vague. “The term now covers every type of discernible Russian activity, from propaganda to conventional warfare, and most that exists in between,” wrote Russia analyst Michael Kofman in March 2016.

Over the past decade, Russia has indeed repeatedly employed tactics associated with hybrid warfare, including a push to target Western audiences with messaging on channels like RT and Sputnik News and with cyber operations such as the use of “troll” accounts. But this was not new even in 2014, and it was something the United States, as well as every other major power, engaged in as well. As early as 2011, the United States was building its own “troll armies” online by developing software to “secretly manipulate social media sites by using fake online personas to influence internet conversations and spread pro-American propaganda.”

“If you torture hybrid warfare long enough, it will tell you anything,” Kofman had admonished, which is precisely what began happening a few months later when Trump critics popularized the idea that a hidden Russian hand was the puppeteer of political developments inside the United States.

The leading voice promoting that claim was a former FBI officer and counterterrorism analyst named Clint Watts. In an article from August 2016, “How Russia Dominates Your Twitter Feed to Promote Lies (And, Trump, Too),” Watts and his co-author, Andrew Weisburd, described how Russia had revived its Cold War-era “Active Measures” campaign, using propaganda and disinformation to influence foreign audiences. As a result, according to the article, Trump voters and Russian propagandists were promoting the same stories on social media that were intended to make America look weak

and incompetent. The authors made the extraordinary claim that the "melding of Russian-friendly accounts and Trumpkins has been going on for some time." If that was true, it meant that anyone expressing support for Donald Trump might be an agent of the Russian government, whether or not the person intended to play that role. It meant that the people they called "Trumpkins," who made up half the country, were attacking America from within. It meant that politics was now war, as it is in many parts of the world, and tens of millions of Americans were the enemy.

Watts made his name as a counterterrorism analyst by studying the social media strategies used by ISIS, but with articles like this, he became the media's go-to expert on Russian trolls and Kremlin disinformation campaigns. It seems he also had powerful backers.

In his book *The Assault on Intelligence,* retired CIA chief Michael Hayden called Watts "the one man, who more than any other was trying to ring the alarm more than two years before the 2016 elections."

Hayden credited Watts in his book with teaching him the power of social media: "Watts pointed out to me that Twitter makes falsehoods seem more believable through sheer repetition and volume. He labeled it a kind of 'computational propaganda.' Twitter in turn drives mainstream media."

A false story algorithmically amplified by Twitter and disseminated by the media—it's no coincidence that this perfectly describes the "bullshit" spread on Twitter about Russian influence operations: In 2017, it was Watts who came up with the idea for the Hamilton 68 dashboard and helped spearhead the initiative.

II. Trump's Election: "It's Facebook's Fault"

No one thought Trump was a normal politician. Being an ogre, Trump horrified millions of Americans who felt a personal betrayal in the possibility that he would occupy the same office held by George Washington and Abe Lincoln. Trump also threatened the business interests of the most powerful sectors of society. It was the latter offense, rather than his putative racism or flagrant un-presidentialness, that sent the ruling class into a state of apoplexy.

Given his focus in office on lowering the corporate tax rate, it's easy to forget that Republican officials and the party's donor class saw Trump as a dangerous radical who threatened their business ties with China, their access to cheap imported labor, and the lucrative business of constant war. But, indeed, that is how they saw him, as reflected in the unprecedented response to Trump's candidacy recorded by *The Wall Street Journal* in September 2016: "No chief executive at the nation's 100 largest companies had donated to Republican Donald Trump's presidential campaign through August, a sharp reversal from 2012, when nearly a third of the CEOs of Fortune 100 companies supported GOP nominee Mitt Romney."

The phenomenon was not unique to Trump. Bernie Sanders, the left-wing populist candidate in 2016, was also seen as a dangerous threat by the ruling class. But whereas the Democrats successfully sabotaged Sanders, Trump made it past his party's gatekeepers, which meant that he had to be dealt with by other means.

Two days after Trump took office, a smirking Senator Chuck Schumer told MSNBC's Rachel Maddow that it was "really dumb" of the new president to get on the bad side of the security agencies that were supposed to work for him: "Let me tell you, you take on the intelligence community, they have six ways from Sunday of getting back at you."

Trump had used sites like Twitter to bypass his party's elites and connect directly with his supporters. Therefore, to cripple the new president and ensure that no one like him could ever come to power again, the intel agencies had to break the independence of the social media platforms. Conveniently, it was the same lesson that many intelligence and defense officials had drawn from the ISIS and Russian campaigns of 2014—namely, that social media was too powerful to be left outside of state control—only applied to domestic politics, which meant the agencies would now have help from politicians who stood to benefit from the effort.

Immediately after the election, Hillary Clinton started blaming Facebook for her loss. Until this point, Facebook and Twitter had tried to remain above the political fray, fearful of jeopardizing potential profits by alienating either party. But now a profound change occurred, as the operation behind the Clinton campaign reoriented itself not simply to reform

the social media platforms, but to conquer them. The lesson they took from Trump's victory was that Facebook and Twitter—more than Michigan and Florida—were the critical battlegrounds where political contests were won or lost. "Many of us are beginning to talk about what a big problem this is," Clinton's chief digital strategist Teddy Goff told Politico the week after the election, referring to Facebook's alleged role in boosting Russian disinformation that helped Trump. "Both from the campaign and from the administration, and just sort of broader Obama orbit…this is one of the things we would like to take on post-election," Goff said.

The press repeated that message so often that it gave the political strategy the appearance of objective validity:

"Donald Trump Won Because of Facebook"; *New York Magazine*, Nov. 9, 2016.

"Facebook, in Cross Hairs After Election, Is Said to Question Its Influence"; *The New York Times*, Nov. 12, 2016.

"Russian propaganda effort helped spread 'fake news' during election, experts say"; *The Washington Post,* Nov. 24, 2016.

"Disinformation, Not Fake News, Got Trump Elected, and It Is Not Stopping"; *The Intercept*, Dec. 6, 2016.

And on it went in countless articles that dominated the news cycle for the next two years.

At first, Facebook's CEO Mark Zuckerberg dismissed the charge that fake news posted on his platform had influenced the outcome of the election as "pretty crazy." But Zuckerberg faced an intense pressure campaign in which every sector of the American ruling class, including his own employees, blamed him for putting a Putin agent in the White House, effectively accusing him of high treason. The final straw came a few weeks after the election when Obama himself "publicly denounced the spread of fake news on Facebook." Two days later, Zuckerberg folded: "Facebook announces new push against fake news after Obama comments."

The false yet foundational claim that Russia hacked the 2016 election provided a justification—just like the claims about weapons of mass destruction that triggered the Iraq War—to plunge America into a wartime state of exception. With the normal rules of constitutional democracy suspended, a coterie of party operatives and security officials then installed a vast, largely invisible new architecture of social control on the backend of the internet's biggest platforms.

Though there was never a public order given, the U.S. government began enforcing martial law online.

Adam Maida

III. Why Do We Need All This Data About People?

The American doctrine of counterinsurgency (COIN) warfare famously calls for "winning hearts and minds." The idea is that victory against insurgent groups depends on gaining the support of the local population, which cannot be accomplished by brute force alone. In places like Vietnam and Iraq, support was secured through a combination of nation-building and appealing to locals by providing them with goods they were presumed to value: money and jobs, for instance, or stability.

Because cultural values vary and what is prized by an Afghan villager may appear worthless to a Swedish accountant, successful counterinsurgents must learn what makes the native population tick. To win over a mind, first you have to get inside it to understand its wants and fears. When that fails, there is another approach in the modern military arsenal to take its place: counterterrorism. Where counterinsurgency tries to win local support, counterterrorism tries to hunt down and kill designated enemies.

Despite the apparent tension in their contrasting approaches, the two strategies have often been used in tandem. Both rely on extensive surveillance networks to gather intelligence on their targets, whether that is figuring out where to dig wells or locating terrorists in order to kill them. But the counterinsurgent in particular imagines that if he can learn enough about a population, it will be possible to reengineer its society. Obtaining answers is just a matter of using the right resources: a combination of surveillance tools and social scientific methods, the joint output of which feeds into all-powerful centralized databases that are believed to contain the totality of the war.

I have observed, reflecting on my experiences as a U.S. Army intelligence officer in Afghanistan, how, "data analytics tools at the fingertips of anyone with access to an operations center or situation room seemed to promise the imminent convergence of map and territory," but ended up becoming a trap as "U.S. forces could measure thousands of different things that we couldn't understand." We tried to cover for that deficit by acquiring even more data. If only we could gather enough information and harmonize it with the correct algorithms, we believed, the database would divine the future.

Not only is that framework foundational in modern American counterinsurgency doctrine, but also it was part of the original impetus for building the internet. The Pentagon built the proto-internet known as ARPANET in 1969 because it needed a decentralized communications infrastructure that could survive nuclear war—but that was not the only goal. The internet, writes Yasha Levine in his history of the subject, *Surveillance Valley,* was also "an attempt to build computer systems that could collect and share intelligence, watch the world in real time, and study and analyze people and political movements with the ultimate goal of predicting and preventing social upheaval. Some even dreamed of creating a sort of early warning radar for human societies: a networked computer system that watched for social and political threats and intercepted them in much the same way that traditional radar did for hostile aircraft."

In the days of the internet "freedom agenda," the popular mythology of Silicon Valley depicted it as a laboratory of freaks, self-starters, free thinkers, and libertarian tinkerers who just wanted to make cool things without the government slowing them down. The alternative history, outlined in Levine's book, highlights that the internet "always had a dual-use nature rooted in intelligence gathering and war." There is truth in both versions, but after 2001 the distinction disappeared.

As Shoshana Zuboff writes in *The Age of Surveillance Capitalism*, at the start of the war on terror "the elective affinity between public intelligence agencies and the fledgling surveillance capitalist Google blossomed in the heat of emergency to produce a unique historical deformity: surveillance exceptionalism."

In Afghanistan, the military had to employ costly drones and "Human Terrain Teams" staffed with adventurous academics to survey the local population and extract their relevant sociological data. But with Americans spending hours a day voluntarily feeding their every thought directly into data monopolies connected to the defense sector, it must have seemed trivially easy for anyone with control of the databases to manipulate the sentiments of the population at home.

More than a decade ago, the Pentagon began funding the development of a host of tools for detecting and countering terrorist messaging on social media. Some were part of a broader "memetic warfare" initiative inside the military that included proposals to weaponize memes to "defeat an enemy ideology and win over the masses of undecided noncombatants." But most of the programs, launched in response to the rise of ISIS and the jihadist group's adept use of social media, focused on scaling up automated means of detecting and censoring terrorist messaging online. Those efforts culminated in January 2016 with the State Department's announcement that it would be opening the aforementioned Global Engagement Center, headed by Michael Lumpkin. Just a few months later, President Obama put the GEC in charge of the new war against disinformation. On the same day that the GEC was announced, Obama and "various high-ranking members of the national security establishment met with representatives from Facebook, Twitter, YouTube, and other Internet powerhouses to discuss how the United States can fight ISIS messaging via social media."

In the wake of the populist upheavals of 2016, leading figures in America's ruling party seized upon the feedback loop of surveillance and control refined through the war on terror as a method for maintaining power inside the United States. Weapons created to fight ISIS and al-Qaeda were turned against Americans who entertained incorrect thoughts about the president or vaccine boosters or gender pronouns or the war in Ukraine.

Former State Department official Mike Benz, who now runs an organization called the Foundation for Freedom Online that bills itself as a digital free-speech watchdog, describes how a company called Graphika, which is "essentially a U.S. Department of Defense-funded censorship consortium" that was created to fight terrorists, was repurposed to censor political speech in America. The company, "initially funded to help do social media counterinsurgency work effectively in conflict zones for the U.S. military," was then "redeployed domestically both on Covid censorship and political censorship," Benz told an interviewer. "Graphika was deployed to monitor social media discourse about Covid and Covid origins, Covid conspiracies, or Covid sorts of issues."

The fight against ISIS morphed into the fight against Trump and "Russian collusion," which morphed into the fight against disinformation. But those were just branding changes; the underlying technological infrastructure and ruling-class philosophy, which claimed the right to remake the world based on a religious sense of expertise, remained unchanged. The human art of politics, which would have required real negotiation and compromise with Trump supporters, was abandoned in favor of a specious science of top-down social engineering that aimed to produce a totally administered society.

For the American ruling class, COIN replaced politics as the proper means of dealing with the natives.

IV. The Internet: From Darling to Demon

Once upon a time, the internet was going to save the world. The first dot-com boom in the 1990s popularized the idea of the internet as a technology for maximizing human potential and spreading democracy. The Clinton administration's 1997 "A Framework for Global Electronic Commerce" put forth the vision: "The Internet is a medium that has tremendous potential for promoting individual freedom and individual empowerment" and "[t]herefore, where possible, the individual should be left in control of the way in which he or she uses this medium." The smart people in the West mocked the naive efforts in other parts of the world to control the flow of information. In 2000, President Clinton scoffed that China's internet crackdown was "like trying to nail Jell-O to the wall." The hype continued through the Bush administration, when internet companies were seen as crucial partners in the state's mass surveillance program and its plan to bring democracy to the Middle East.

But the hype really went into overdrive when President Obama was elected through a "big data"-driven campaign that prioritized social media outreach. There appeared to be a genuine philosophical alignment between Obama's political style as the "Hope" and "Change" president whose guiding principle in foreign policy was "Don't do dumb shit" and the internet search company whose original motto was "Do no evil." There were also deep personal ties connecting the two powers, with 252 cases over the course of Obama's presidency of people moving between jobs at the White House and Google. From 2009 to 2015, White House and Google employees were meeting, on average, more than once a week.

As Obama's secretary of state, Hillary Clinton led the government's "Internet freedom" agenda, which aimed to "promote online communications as a tool for opening up closed societies." In a speech from 2010, Clinton issued a warning about the spread of digital censorship in authoritarian regimes: "A new information curtain is descending across much of the world," she said. "And beyond this partition, viral videos and blog posts are becoming the samizdat of our day."

It is a supreme irony that the very people who a decade ago led the freedom agenda for other countries have since pushed the United States to implement one of the largest and most powerful censorship machines in existence under the guise of fighting disinformation.

Or perhaps *irony* is not the right word to capture the difference between the freedom-loving Clinton of a decade ago and the pro-censorship activist of today, but it gets at what appears to be the about-face done by a class of people who were public standard-bearers for radically different ideas barely 10 years earlier. These people—politicians, first and foremost—saw (and presented) internet freedom as a positive force for humanity when it empowered them and served their interests, but as something demonic when it broke down those hierarchies of power and benefited their opponents. That's how to bridge the gap between the Hillary Clinton of 2013 and the Clinton of 2023: Both see the internet as an immensely powerful tool for driving political processes and effecting regime change.

Which is why, in the Clinton and Obama worlds, the rise of Donald Trump looked like a profound betrayal—because, as they saw it, Silicon Valley could have stopped it but didn't. As heads of the government's internet policy, they had helped the tech companies build their fortunes on mass surveillance and evangelized the internet as a beacon of freedom and progress while turning a blind eye to their flagrant violations of antitrust statutes. In return, the tech companies had done the unthinkable—not because they had allowed Russia to "hack the election," which was a desperate accusation thrown out to mask the stench of failure, but because they refused to intervene to prevent Donald Trump from winning.

In his book *Who Owns the Future?*, tech pioneer Jaron Lanier writes, "The primary business of digital networking has come to be the creation of ultra-secret mega-dossiers about what others are doing, and using this information to concentrate money and power." Because digital economies produce ever-greater concentrations of data and power, the inevitable happened: The tech companies got too powerful.

What could the leaders of the ruling party do? They had two options. They could use the government's regulatory power to counter-attack: Break up the data monopolies and restructure the social contract underwriting the internet so that individuals retained ownership of their data instead of having it ripped off every time they clicked into a public commons. Or, they could preserve the tech companies' power while forcing them to drop the pretense of neutrality and instead line up behind the ruling party—a tempting prospect, given what they could do with all that power.

They chose option B.

Declaring the platforms guilty of electing Trump—a candidate every bit as loathsome to the highly educated elites in Silicon Valley as he was to the highly educated elites in New York and D.C.—provided the club that the media and the political class used to beat the tech companies into becoming more powerful and more obedient.

V. Russiagate! Russiagate! Russiagate!

If one imagines that the American ruling class faced a problem—Donald Trump appeared to threaten their institutional survival—then the Russia investigation didn't just provide the means to unite the various branches of that class, in and out of government, against a common foe. It also gave them the ultimate form of leverage over the most powerful non-aligned sector of society: the tech industry. The coordination necessary to carry out the Russian collusion frame-up was the vehicle, fusing (1) the political goals of the Democratic Party, (2) the institutional agenda of the intelligence and security agencies, and (3) the narrative power and moral fervor of the media with (4) the tech companies' surveillance architecture.

The secret FISA warrant that allowed U.S. security agencies to begin spying on the Trump campaign was based on the Steele dossier, a partisan hatchet job paid for by Hillary Clinton's team that consisted of provably false reports alleging a working relationship between Donald Trump and the Russian government. While a powerful short-term weapon against Trump, the dossier was also obvious bullshit, which suggested it might eventually become a liability.

Disinformation solved that problem while placing a nuclear-grade weapon in the arsenal of the anti-Trump resistance. In the beginning, disinformation had been only one among a half-dozen talking points coming from the anti-Trump camp. It won out over the others because it was capable of explaining anything and everything yet simultaneously remained so ambiguous it could not be disproved. Defensively, it provided a means to attack and discredit anyone who questioned the dossier or the larger claim that Trump colluded with Russia.

All the old McCarthyite tricks were new again. *The Washington Post* aggressively trumpeted the claim that disinformation swung the 2016 election, a crusade that began within days of Trump's victory, with the article "Russian propaganda effort helped spread 'fake news' during election, experts say." (The lead expert quoted in the article: Clint Watts.)

A steady flow of leaks from intelligence officials to national security reporters had already established the false narrative that there was credible evidence of collusion between the Trump campaign and the Kremlin. When Trump won in spite of those reports, the senior officials responsible for spreading them, most notably CIA chief John Brennan, doubled down on their claims. Two weeks before Trump took office, the Obama administration released a declassified version of an intelligence community assessment, known as an ICA, on "Russian Activities and Intentions in Recent Elections," which asserted that "Putin and the Russian government developed a clear preference for President-elect Trump."

The ICA was presented as the objective, nonpolitical consensus reached by multiple intelligence agencies. In the *Columbia Journalism Review*, Jeff Gerth writes that the assessment received "massive, and largely uncritical coverage" in the press. But, in fact, the ICA was just the opposite: a selectively curated political document that deliberately omitted contrary evidence to create the impression that the collusion narrative was not a widely disputed rumor, but an objective fact.

A classified report by the House Intelligence Committee on the creation of the ICA detailed just how unusual and nakedly political it was. "It wasn't 17 agencies, and it wasn't even a dozen analysts from the three agencies who wrote the assessment," a senior intelligence official who read a draft version of the House report told the journalist Paul Sperry. "It was just five officers of the CIA who wrote it, and Brennan handpicked all five. And the lead writer was a good friend of Brennan's." An Obama appointee, Brennan had broken with precedent by weighing in on politics while serving as CIA director. That set the stage for his post-government career as an MSNBC analyst and "resistance" figure who made headlines by accusing Trump of treason.

Mike Pompeo, who succeeded Brennan at the CIA, said that as the agency's director, he learned that "senior analysts who had been working on Russia for nearly their entire careers were made bystanders" when the ICA was being written. According to Sperry, Brennan "excluded conflicting evidence about Putin's motives from the report, despite objections from some intelligence analysts who argued Putin counted on Clinton winning the election and viewed Trump as a 'wild card.'" (Brennan was also the one who overrode the objections of other agencies to include the Steele dossier as part of the official assessment.)

Despite its irregularities, the ICA worked as intended: Trump began his presidency under a cloud of suspicion that he was never able to dispel. Just as Schumer promised, the intelligence officials wasted no time in taking their revenge.

And not only revenge, but also forward-planning action. The claim that Russia hacked the 2016 vote allowed federal agencies to implement the new public-private censorship machinery under the pretext of ensuring "election integrity." People who expressed true and constitutionally protected opinions about the 2016 election (and later about issues like COVID-19 and the U.S. withdrawal from Afghanistan) were labeled un-American, racists, conspiracists, and stooges of Vladimir Putin and systematically removed from the digital public square to prevent their ideas from spreading

disinformation. By an extremely conservative estimate based on public reporting, there have been tens of millions of such cases of censorship since Trump's election.

And here's the climax of this particular entry: On Jan. 6, 2017—the same day that Brennan's ICA report lent institutional backing to the false claim that Putin helped Trump—Jeh Johnson, the outgoing Obama-appointed secretary of the Department of Homeland Security, announced that, in response to Russian electoral interference, he had designated U.S. election systems as "critical national infrastructure." The move placed the property of 8,000 election jurisdictions across the country under the control of the DHS. It was a coup that Johnson had been attempting to pull off since the summer of 2016, but that, as he explained in a later speech, was blocked by local stakeholders who told him "that running elections in this country was the sovereign and exclusive responsibility of the states, and they did not want federal intrusion, a federal takeover, or federal regulation of that process." So Johnson found a work-around by unilaterally rushing the measure through in his last days in office.

It's clear now why Johnson was in such a rush: Within a few years, all of the claims used to justify the extraordinary federal seizure of the country's electoral system would fall apart. In July 2019 the Mueller report concluded that Donald Trump did not collude with the Russian government—the same conclusion reached by the inspector general's report into the origins of the Trump-Russia probe, released later that year. Finally, on Jan. 9, 2023, *The Washington Post* quietly published an addendum in its cybersecurity newsletter about New York University's Center for Social Media and Politics study. Its conclusion: "Russian trolls on Twitter had little influence on 2016 voters."

But by then it didn't matter. In the final two weeks of the Obama administration, the new counter-disinformation apparatus scored one of its most significant victories: the power to directly oversee federal elections that would have profound consequences for the 2020 contest between Trump and Joe Biden.

VI. Why the Post-9/11 "War on Terror" Never Ended

Clint Watts, who headed up the Hamilton 68 initiative, and Michael Hayden, the former Air Force general, CIA chief, and NSA director who championed Watts, are both veterans of the U.S. counterterrorism establishment. Hayden ranks among the most senior intelligence officers the United States has ever produced and was a principal architect of the post-9/11 mass surveillance system. Indeed, an astounding percentage of the key figures in the counter-disinformation complex cut their teeth in the worlds of counterterrorism and counterinsurgency warfare.

Michael Lumpkin, who headed the GEC, the State Department agency that served as the first command center in the war against disinformation, is a former Navy SEAL with a counterterrorism background. The GEC itself grew out of the Center for Strategic Counterterrorism Communications before being repurposed to fight disinformation.

Twitter had the chance to stop the Hamilton 68 hoax before it got out of hand, yet chose not to. Why? The answer can be seen in the emails sent by a Twitter executive named Emily Horne, who advised against calling out the scam. Twitter had a smoking gun showing that the Alliance for Securing Democracy, the neoliberal think tank behind the Hamilton 68 initiative, was guilty of exactly the charge it made against others: peddling disinformation that inflamed domestic political divisions and undermined the legitimacy of democratic institutions. But that had to be weighed against other factors, Horne suggested, such as the need to stay on the good side of a powerful organization. "We have to be careful in how much we push back on ASD publicly," she wrote in February 2018.

The ASD was lucky to have someone like Horne on the inside of Twitter. Then again, maybe it wasn't luck. Horne had previously worked at the State Department, handling the "digital media and think tank outreach" portfolio. According to her LinkedIn, she "worked closely with foreign policy reporters covering [ISIS] … and executed communications plans relating to Counter-[ISIS] Coalition activities." Put another way, she had a background in counterterrorism operations similar to Watts' but with more of an emphasis on spinning the press and civil society groups. From there she became the director for strategic communications for Obama's National Security Council, only leaving to join Twitter in June 2017. Sharpen the focus on that timeline, and here's what it shows: Horne joined Twitter one month before the launch of

ASD, just in time to advocate for protecting a group run by the kind of power brokers who held the keys to her professional future.

It is no coincidence that the war against disinformation began at the very moment the Global War on Terror (GWOT) finally appeared to be coming to an end. Over two decades, the GWOT fulfilled President Dwight Eisenhower's warnings about the rise of a military-industrial complex with "unwarranted influence." It evolved into a self-interested, self-justifying industry that employed thousands of people in and out of government who operated without clear oversight or strategic utility. It might have been possible for the U.S. security establishment to declare victory and move from a permanent war footing to a peacetime posture, but as one former White House national security official explained to me, that was unlikely. "If you work in counterterrorism," the former official said, "there's no incentive to ever say that you're winning, kicking their ass, and they're a bunch of losers. It's all about hyping a threat." He described "huge incentives to inflate the threat" that have been internalized in the culture of the U.S. defense establishment and are "of a nature that they don't require one to be particularly craven or intellectually dishonest."

"This huge machinery was built around the war on terror," the official said. "A massive infrastructure that includes the intelligence world, all the elements of DoD, including the combatant commands, CIA and FBI and all the other agencies. And then there are all the private contractors and the demand in think tanks. I mean, there are billions and billions of dollars at stake."

The seamless transition from the war on terror to the war on disinformation was thus, in large measure, simply a matter of professional self-preservation. But it was not enough to sustain the previous system; to survive, it needed to continually raise the threat level.

In the months after the attacks of Sept. 11, 2001, George W. Bush promised to drain the swamps of radicalism in the Middle East. Only by making the region safe for democracy, Bush said, could he ensure that it would stop producing violent jihadists like Osama bin Laden.

Today, to keep America safe, it is no longer enough to invade the Middle East and bring its people democracy. According to the Biden White House and the army of disinformation experts, the threat is now coming from within. A network of right-wing domestic extremists, QAnon fanatics, and white nationalists is supported by a far larger population of some 70 million Trump voters whose political sympathies amount to a fifth column within the United States. But how did these people get radicalized into accepting the bitter and destructive white jihad of Trumpist ideology? Through the internet, of course, where the tech companies, by refusing to "do more" to combat the scourge of hate speech and fake news, allowed toxic disinformation to poison users' minds.

After 9/11, the threat of terrorism was used to justify measures like the Patriot Act that suspended constitutional rights and placed millions of Americans under a shadow of mass surveillance. Those policies were once controversial but have come to be accepted as the natural prerogatives of state power. As journalist Glenn Greenwald observed, George W. Bush's "'with-us-or-with-the-terrorists' directive provoked a fair amount of outrage at the time but is now the prevailing mentality within U.S. liberalism and the broader Democratic Party."

The war on terror was a dismal failure that ended with the Taliban returning to power in Afghanistan. It also became deeply unpopular with the public. Why, then, would Americans choose to empower the leaders and sages of that war to be the stewards of an even more expansive war against disinformation? It is possible to venture a guess: Americans did not choose them. Americans are no longer presumed to have the right to choose their own leaders or to question decisions made in the name of national security. Anyone who says otherwise can be labeled a domestic extremist.

VII. The Rise of "Domestic Extremists"

A few weeks after Trump supporters rioted in the U.S. Capitol on Jan. 6, 2021, former director of the CIA's Counterterrorism Center Robert Grenier wrote an article for *The New York Times* advocating for the United States to wage a "comprehensive counterinsurgency program" against its own citizens.

Counterinsurgency, as Grenier would know, is not a limited, surgical operation but a broad effort conducted across an entire society that inevitably involves collateral destruction. Targeting only the most violent extremists who attacked law enforcement officers at the Capitol would not be enough to defeat the insurgency. Victory would require winning the hearts and minds of the natives—in this case, the Christian dead-enders and rural populists radicalized by their grievances into embracing the Bin Laden-like cult of MAGA. Lucky for the government, there is a cadre of experts who are available to deal with this difficult problem: people like Grenier, who now works as a consultant in the private-sector counterterrorism industry, where he has been employed since leaving the CIA.

Of course there are violent extremists in America, as there have always been. However, if anything, the problem is less severe now than it was in the 1960s and 1970s, when political violence was more common. Exaggerated claims about a new breed of domestic extremism so dangerous it cannot be handled through existing laws, including domestic terrorism statutes, is itself a product of the U.S.-led information war, which has effaced the difference between speech and action.

"Civil wars don't start with gunshots. They start with words," Clint Watts proclaimed in 2017 when he testified before Congress. "America's war with itself has already begun. We all must act now on the social media battlefield to quell information rebellions that can quickly lead to violent confrontations." Watts is a career veteran of military and government service who seems to share the belief, common among his colleagues, that once the internet entered its populist stage and threatened entrenched hierarchies, it became a grave danger to civilization. But this was a fearful response, informed by beliefs widely, and no doubt sincerely, shared in the Beltway that mistook an equally sincere populist backlash termed "the revolt of the public" by former CIA analyst Martin Gurri for an act of war. The standard Watts and others introduced, which quickly became the elite consensus, treats tweets and memes—the primary weapons of disinformation—as acts of war.

Using the hazy category of disinformation allowed security experts to conflate racist memes with mass shootings in Pittsburgh and Buffalo and with violent protests like the one that took place at the Capitol. It was a rubric for catastrophizing speech and maintaining a permanent state of fear and emergency. And it received the full backing of the Pentagon, the intelligence community, and President Biden, all of whom, notes Glenn Greenwald, have declared that "the gravest menace to American national security" is not Russia, ISIS, China, Iran, or North Korea, but "'domestic extremists' in general—and far-right white supremacist groups in particular."

The Biden administration has steadily expanded domestic terrorism and counter-extremism programs. In February 2021, DHS officials announced that they had received additional funding to boost department-wide efforts at "preventing domestic terrorism," including an initiative to counter the spread of disinformation online, which uses an approach seemingly borrowed from the Soviet handbook, called "attitudinal inoculation."

Adam Maida

VIII. The NGO Borg

In November 2018, Harvard Kennedy School's Shorenstein Center on Media Politics and Public Policy published a study titled "The Fight Against Disinformation in the U.S.: A Landscape Analysis." The scope of the paper is comprehensive, but its authors are especially focused on the centrality of philanthropically funded nonprofit organizations and their relationship to the media. The Shorenstein Center is a key node in the complex the paper describes, giving the authors' observations an insider's perspective.

"In this landscape analysis, it became apparent that a number of key advocates swooping in to save journalism are not corporations or platforms or the U.S. government, but rather foundations and philanthropists who fear the loss of a free press and the underpinning of a healthy society. ... With none of the authoritative players—the government and platforms who push the content—stepping up to solve the problem quickly enough, the onus has fallen on a collective effort by newsrooms, universities, and foundations to flag what is authentic and what is not."

To save journalism, to save democracy itself, Americans should count on the foundations and philanthropists—people like eBay founder Pierre Omidyar, Open Society Foundations' George Soros, and internet entrepreneur and Democratic Party fundraiser Reid Hoffman. In other words, Americans were being asked to rely on private billionaires who were pumping billions of dollars into civic organizations—through which they would influence the American political process.

There is no reason to question the motivations of the staffers at these NGOs, most of whom were no doubt perfectly sincere in the conviction that their work was restoring the "underpinning of a healthy society." But certain observations can be made about the nature of that work. First, it placed them in a position below the billionaire philanthropists but above hundreds of millions of Americans whom they would guide and instruct as a new information clerisy by separating truth from falsehood, as wheat from chaff. Second, this mandate, and the enormous funding behind it, opened up thousands of new jobs for information regulators at a moment when traditional journalism was collapsing. Third, the first two points placed the immediate self-interest of the NGO staffers perfectly in line with the imperatives of the American ruling party and security state. In effect, a concept taken from the worlds of espionage and warfare—disinformation—was seeded into academic and nonprofit spaces, where it ballooned into a pseudoscience that was used as an instrument of partisan warfare.

Virtually overnight, the "whole of society" national mobilization to defeat disinformation that Obama initiated led to the creation and credentialing of a whole new class of experts and regulators.

The modern "fact-checking" industry, for instance, which impersonates a well-established scientific field, is in reality a nakedly partisan cadre of compliance officers for the Democratic Party. Its leading organization, the International Fact-Checking Network, was established in 2015 by the Poynter Institute, a central hub in the counter-disinformation complex.

Everywhere one looks now, there is a disinformation expert. They are found at every major media publication, in every branch of government, and in academic departments, crowding each other out on cable news programs, and of course staffing the NGOs. There is enough money coming from the counter-disinformation mobilization to both fund new organizations and convince established ones like the Anti-Defamation League to parrot the new slogans and get in on the action.

How is it that so many people could suddenly become experts in a field—"disinformation"—that not 1 in 10,000 of them could have defined in 2014? Because expertise in disinformation involves ideological orientation, not technical knowledge. For proof, look no further than the arc traced by Prince Harry and Meghan Markle, who pivoted from being failed podcast hosts to joining the Aspen Institute's Commission on Information Disorder. Such initiatives flourished in the years after Trump and Brexit.

But it went beyond celebrities. According to former State Department official Mike Benz, "To create a 'whole of society' consensus on the censorship of political opinions online that were 'casting doubt' ahead of the 2020 election, DHS organized 'disinformation' conferences to bring together tech companies, civil society groups, and news media to all build consensus—with DHS prodding (which is meaningful: many partners receive government funds through grants or contracts, or fear government regulatory or retaliatory threats)—on expanding social media censorship policies."

A DHS memo, first made public by journalist Lee Fang, describes a DHS official's comment "during an internal strategy discussion, that the agency should use third-party nonprofits as a "clearing house for information to avoid the appearance of government propaganda."

It is not unusual that a government agency would want to work with private corporations and civil society groups, but in this case the result was to break the independence of organizations that should have been critically investigating the government's efforts. The institutions that claim to act as watchdogs on government power rented themselves out as vehicles for manufacturing consensus.

Perhaps it is not a coincidence that the fields that have been most aggressive in cheerleading the war against disinformation and calling for greater censorship—counterterrorism, journalism, epidemiology—share a public record of spectacular failure in recent years. The new information regulators failed to win over vaccine skeptics, convince MAGA diehards that the 2020 election was legitimate, or prevent the public from inquiring into the origins of the COVID-19 pandemic, as they tried desperately to do.

But they succeeded in galvanizing a wildly lucrative whole-of-society effort, providing thousands of new careers and a renewed mandate of heaven to the institutionalists who saw populism as the end of civilization.

IX. COVID-19

By 2020, the counter-disinformation machine had grown into one of the most powerful forces in American society. Then the COVID-19 pandemic dumped jet fuel into its engine. In addition to fighting foreign threats and deterring domestic extremists, censoring "deadly disinformation" became an urgent need. To take just one example, Google's censorship, which applied to its subsidiary sites like YouTube, called for "removing information that is problematic" and "anything that would go against World Health Organization recommendations"—a category that at different points in the constantly evolving narrative would have included wearing masks, implementing travel bans, saying that the virus is highly contagious, and suggesting it might have come from a laboratory.

President Biden publicly accused social media companies of "killing people" by not censoring enough vaccine disinformation. Using its new powers and direct channels inside the tech companies, the White House began sending lists of people it wanted banned, such as journalist Alex Berenson. Berenson was kicked off Twitter after tweeting that mRNA vaccines don't "stop infection. Or transmission." As it turned out, that was a true statement. The health authorities at the time were either misinformed or lying about the vaccines' ability to prevent the spread of the virus. In fact, despite claims from the health authorities and political officials, the people in charge of the vaccine knew this all along. In the record of a meeting in December 2020, Food and Drug Administration adviser Dr. Patrick Moore stated, "Pfizer has presented no evidence in its data today that the vaccine has any effect on virus carriage or shedding, which is the fundamental basis for herd immunity."

Dystopian in principle, the response to the pandemic was also totalitarian in practice. In the United States, the DHS produced a video in 2021 encouraging "children to report their own family members to Facebook for 'disinformation' if they challenge US government narratives on Covid-19."

"Due to both the pandemic and the disinformation about the election, there are increasing numbers of what extremism experts call 'vulnerable individuals' who could be radicalized," warned Elizabeth Neumann, former assistant secretary of Homeland Security for Counterterrorism and Threat Reduction, on the one-year anniversary of the Capitol riots.

Klaus Schwab, head of the World Economic Forum and *capo di tutti capi* of the global expert class, saw the pandemic as an opportunity to implement a "Great Reset" that could advance the cause of planetary information control: "The containment of the coronavirus pandemic will necessitate a global surveillance network capable of identifying new outbreaks as soon as they arise."

X. Hunter's Laptops: The Exception to the Rule

The laptops are real. The FBI has known this since 2019, when it first took possession of them. When the *New York Post* attempted to report on them, dozens of the most senior national security officials in the United States lied to the public, claiming the laptops were likely part of a Russian "disinformation" plot. Twitter, Facebook, and Google, operating as fully integrated branches of the state security infrastructure, carried out the government's censorship orders based on that lie. The press swallowed the lie and cheered on the censorship.

The story of the laptops has been framed as many things, but the most fundamental truth about it is that it was the successful culmination of the yearslong effort to create a shadow regulatory bureaucracy built specifically to prevent a repeat of Trump's 2016 victory.

It may be impossible to know exactly what effect the ban on reporting about Hunter Biden's laptops had on the 2020 vote, but the story was clearly seen as threatening enough to warrant an openly authoritarian attack on the independence of the press. The damage to the country's underlying social fabric, in which paranoia and conspiracy have been normalized, is incalculable. As recently as February, Rep. Alexandria Ocasio-Cortez referred to the scandal as the "half-fake laptop story" and as "an embarrassment," months after even the Bidens had been forced to acknowledge that the story is authentic.

While the laptop is the best-known case of the ruling party's intervention in the Trump-Biden race, its brazenness was an exception. The vast majority of the interference in the election was invisible to the public and took place through censorship mechanisms carried out under the auspices of "election integrity." The legal framework for this had been put in place shortly after Trump took office, when the outgoing DHS chief Jeh Johnson passed an 11th-hour rule—over the vehement objections of local stakeholders—declaring election systems to be critical national infrastructure, thereby placing them under the supervision of the agency. Many observers had expected that the act would be repealed by Johnson's successor, Trump-appointed John Kelly, but curiously it was left in place.

In 2018, Congress created a new agency inside of the DHS called the Cybersecurity and Infrastructure Security Agency (CISA) that was tasked with defending America's infrastructure—now including its election systems—from foreign attacks. In 2019, the DHS added another agency, the Foreign Influence and Interference Branch, which was focused on countering foreign disinformation. As if by design, the two roles merged. Russian hacking and other malign foreign-information attacks were said to threaten U.S. elections. But, of course, none of the officials in charge of these departments could say with certainty whether a particular claim was foreign disinformation, simply wrong, or merely inconvenient. Nina Jankowicz, the pick to lead the DHS's short-lived Disinformation Governance Board, lamented the problem in her book *How to Lose the Information War: Russia, Fake News and the Future of Conflict.* "What makes this information war so difficult to win," she wrote, "is not just the online tools that amplify and target its messages or the adversary that is sending them; it's the fact that those messages are often unwittingly delivered not by trolls or bots, but by authentic local voices."

The latitude inherent in the concept of disinformation enabled the claim that preventing electoral sabotage required censoring Americans' political views, lest an idea be shared in public that was originally planted by foreign agents.

In January 2021, CISA "transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM [ed. note: an acronym for *misinformation, disinformation, and malinformation*]," according to an August 2022 report from the DHS's Office of Inspector General. After the pretense of fighting a foreign threat fell away, what was left was the core mission to enforce a narrative monopoly over truth.

The new domestic-focused task force was staffed by 15 employees dedicated to finding "all types of disinformation"—but specifically that which related to "elections and critical infrastructure"—and being "responsive to current events," a euphemism for promoting the official line of divisive issues, as was the case with the "COVID-19 Disinformation Toolkit" released to "raise awareness related to the pandemic."

Kept a secret from the public, the switch was "plotted on DHS's own livestreams and internal documents," according to Mike Benz. "DHS insiders' collective justification, without uttering a peep about the switch's revolutionary implications, was that 'domestic disinformation' was now a greater 'cyber threat to elections' than falsehoods flowing from foreign interference."

Just like that, without any public announcements or black helicopters flying in formation to herald the change, America had its own ministry of truth.

Together they operated an industrial-scale censorship machine in which the government and NGOs sent tickets to the tech companies that flagged objectionable content they wanted scrubbed. That structure allowed the DHS to outsource its work to the Election Integrity Project (EIP), a consortium of four groups: the Stanford Internet Observatory; private anti-disinformation company Graphika (which had formerly been employed by the Defense Department against groups like ISIS in the war on terror); Washington University's Center for an Informed Public; and the Atlantic Council's Digital Forensics Research Lab. Founded in 2020 in partnership with the DHS, the EIP served as the government's "deputized domestic disinformation flagger," according to congressional testimony from journalist Michael Shellenberger, who notes that the EIP claims it classified more than 20 million unique "misinformation incidents" between Aug. 15 and Dec. 12, 2020. As EIP head Alex Stamos explained, this was a work-around for the problem that the government "lacked both kinda the funding and the legal authorizations."

Looking at the censorship figures that the DHS's own partners reported for the 2020 election cycle in their internal audits, the Foundation for Freedom Online summarized the scope of the censorship campaign in seven bullet points:

- 22 million tweets labeled "misinformation" on Twitter;
- 859 million tweets collected in databases for "misinformation" analysis;
- 120 analysts monitoring social media "misinformation" in up to 20-hour shifts;
- 15 tech platforms monitored for "misinformation," often in real-time;
- <1 hour average response time between government partners and tech platforms;
- Dozens of "misinformation narratives" targeted for platform-wide throttling; and
- Hundreds of millions of individual Facebook posts, YouTube videos, TikToks, and tweets impacted due to "misinformation" Terms of Service policy changes, an effort DHS partners openly plotted and bragged that tech companies would never have done without DHS partner insistence and "huge regulatory pressure" from government.

XI. The New One-Party State

In February 2021, a long article in *Time* magazine by journalist Molly Ball celebrated the "Shadow Campaign That Saved the 2020 Election." Biden's victory, wrote Ball, was the result of a "conspiracy unfolding behind the scenes" that drew together "a vast, cross-partisan campaign to protect the election" in an "extraordinary shadow effort." Among the many accomplishments of the heroic conspirators, Ball notes, they "successfully pressured social media companies to take a harder line against disinformation and used data-driven strategies to fight viral smears." It is an incredible article, like an entry from the crime blotter that somehow got slipped into the society pages, a paean to the saviors of democracy that describes in detail how they dismembered it.

Not so long ago, talk of a "deep state" was enough to mark a person as a dangerous conspiracy theorist to be summarily flagged for monitoring and censorship. But language and attitudes evolve, and today the term has been cheekily reappropriated by supporters of the deep state. For instance, a new book, *American Resistance*, by neoliberal national security analyst David Rothkopf, is subtitled *The Inside Story of How the Deep State Saved the Nation*.

The deep state refers to the power wielded by unelected government functionaries and their paragovernmental adjuncts who have administrative power to override the official, legal procedures of a government. But a ruling class describes a social group whose members are bound together by something deeper than institutional position: their shared values and instincts. While the term is often used loosely and sometimes as a pejorative rather than a descriptive label, in fact the American ruling class can be simply and straightforwardly defined.

Two criteria define membership in the ruling class. First, as Michael Lind has written, it is made up of people who belong to a "homogeneous national oligarchy, with the same accent, manners, values, and educational backgrounds from Boston to Austin and San Francisco to New York and Atlanta." America has always had regional elites; what is unique about the present is the consolidation of a single, national ruling class.

Second, to be a member of the ruling class is to believe that only other members of your class can be allowed to lead the country. That is to say, members of the ruling class refuse to submit to the authority of anyone outside the group, whom they disqualify from eligibility by casting them as in some way illegitimate.

Faced with an external threat in the form of Trumpism, the natural cohesion and self-organizing dynamics of the social class were fortified by new top-down structures of coordination that were the goal and the result of Obama's national mobilization. In the run-up to the 2020 election, according to reporting by Lee Fang and Ken Klippenstein for The Intercept, "tech companies including Twitter, Facebook, Reddit, Discord, Wikipedia, Microsoft, LinkedIn, and Verizon Media met on a monthly basis with the FBI, CISA, and other government representatives … to discuss how firms would handle misinformation during the election."

Historian Angelo Codevilla, who popularized the concept of an American "ruling class" in a 2010 essay and then became its primary chronicler, saw the new, national aristocracy as an outgrowth of the opaque power acquired by the U.S. security agencies. "The bipartisan ruling class that grew in the Cold War, who imagined themselves and who managed to be regarded as entitled by expertise to conduct America's business of war and peace, protected its status against a public from which it continued to diverge by translating the commonsense business of war and peace into a private, pseudo-technical language impenetrable to the uninitiated," he wrote in his 2014 book, *To Make and Keep Peace Among Ourselves and with All Nations*.

What do the members of the ruling class believe? They believe, I argue, "in informational and management solutions to existential problems" and in their "own providential destiny and that of people like them to rule, regardless of their failures." As a class, their highest principle is that they alone can wield power. If any other group were to rule, all progress and hope would be lost, and the dark forces of fascism and barbarism would at once sweep back over the earth. While technically an opposition party is still permitted to exist in the United States, the last time it attempted to govern nationally, it was subjected to a yearslong coup. In effect, any challenge to the authority of the ruling party, which represents the interests of the ruling class, is depicted as an existential threat to civilization.

An admirably direct articulation of this outlook was provided recently by famous atheist Sam Harris. Throughout the 2010s, Harris' higher-level rationalism made him a star on YouTube, where thousands of videos showcased him "owning" and "pwning" religious opponents in debates. Then Trump arrived. Harris, like so many others who saw in the former president a threat to all that was good in the world, abandoned his principled commitment to the truth and became a defender of propaganda.

In a podcast appearance last year, Harris acknowledged the politically motivated censorship of reporting related to Hunter Biden's laptops and admitted "a left-wing conspiracy to deny the presidency to Donald Trump." But, echoing Ball, he declared this a good thing.

“I don’t care what’s in the Hunter Biden laptop. … Hunter Biden could have had corpses of children in his basement, and I would not have cared,” Harris told his interviewers. He could overlook the murdered children because an even greater danger lurked in the possibility of Trump’s reelection, which Harris compared to “an asteroid hurtling toward Earth.”

With an asteroid hurtling toward Earth, even the most principled rationalists might end up asking for safety over truth. But an asteroid has been falling toward Earth every week for years now. The pattern in these cases is that the ruling class justifies taking liberties with the law to save the planet but ends up violating the Constitution to hide the truth and protect itself.

XII. The End of Censorship

The public’s glimpses into the early stages of the transformation of America from democracy to digital leviathan are the result of lawsuits and FOIAs—information that had to be pried from the security state—and one lucky fluke. If Elon Musk had not decided to purchase Twitter, many of the crucial details in the history of American politics in the Trump era would have remained secret, possibly forever.

But the system reflected in those disclosures may well be on its way out. It is already possible to see how the kind of mass censorship practiced by the EIP, which requires considerable human labor and leaves behind plenty of evidence, could be replaced by artificial intelligence programs that use the information about targets accumulated in behavioral surveillance dossiers to manage their perceptions. The ultimate goal would be to recalibrate people’s experiences online through subtle manipulations of what they see in their search results and on their feed. The aim of such a scenario might be to prevent censor-worthy material from being produced in the first place.

In fact, that sounds rather similar to what Google is already doing in Germany, where the company recently unveiled a new campaign to expand its “prebunking” initiative “that aims to make people more resilient to the corrosive effects of online misinformation,” according to the Associated Press. The announcement closely followed Microsoft founder Bill Gates’ appearance on a German podcast, during which he called for using artificial intelligence to combat “conspiracy theories” and “political polarization.” Meta has its own prebunking program. In a statement to the website Just The News, Mike Benz called prebunking “a form of narrative censorship integrated into social media algorithms to stop citizens from forming specific social and political belief systems” and compared it to the “pre-crime” featured in dystopian science-fiction movie *Minority Report*.

Meanwhile, the military is developing weaponized AI technology to dominate the information space. According to USASpending.gov, an official government website, the two largest contracts related to disinformation came from the Department of Defense to fund technologies for automatically detecting and defending against large-scale disinformation attacks. The first, for $11.9 million, was awarded in June 2020 to PAR Government Systems Corporation, a defense contractor in upstate New York. The second, issued in July 2020 for $10.9 million, went to a company called SRI International.

SRI International was originally connected to Stanford University before splitting off in the 1970s, a relevant detail considering that the Stanford Internet Observatory, an institution still directly connected to the school, led 2020’s EIP, which might well have been the largest mass censorship event in world history—a capstone of sorts to the record of pre-AI censorship.

Then there is the work going on at the National Science Foundation, a government agency that funds research in universities and private institutions. The NSF has its own program called the Convergence Accelerator Track F, which is helping to incubate a dozen automated disinformation-detection technologies explicitly designed to monitor issues like “vaccine hesitancy and electoral skepticism.”

“One of the most disturbing aspects” of the program, according to Benz, “is how similar they are to military-grade social media network censorship and monitoring tools developed by the Pentagon for the counterinsurgency and counterterrorism contexts abroad.”

In March, the NSF's chief information officer, Dorothy Aronson, announced that the agency was "building a set of use cases" to explore how it could employ ChatGPT, the AI language model capable of a reasonable simulation of human speech, to further automate the production and dissemination of state propaganda.

The first great battles of the information war are over. They were waged by a class of journalists, retired generals, spies, Democratic Party bosses, party apparatchiks, and counterterrorism experts against the remnant of the American people who refused to submit to their authority.

Future battles fought through AI technologies will be harder to see.

XIII. After Democracy

Less than three weeks before the 2020 presidential election, *The New York Times* published an important article titled "The First Amendment in the age of disinformation." The essay's author, *Times* staff writer and Yale Law School graduate Emily Bazelon, argued that the United States was "in the midst of an information crisis caused by the spread of viral disinformation" that she compares to the "catastrophic" health effects of the novel coronavirus. She quotes from a book by Yale philosopher Jason Stanley and linguist David Beaver: "Free speech threatens democracy as much as it also provides for its flourishing."

So the problem of disinformation is also a problem of democracy itself—specifically, that there's too much of it. To save liberal democracy, the experts prescribed two critical steps: America must become less free and less democratic. This necessary evolution will mean shutting out the voices of certain rabble-rousers in the online crowd who have forfeited the privilege of speaking freely. It will require following the wisdom of disinformation experts and outgrowing our parochial attachment to the Bill of Rights. This view may be jarring to people who are still attached to the American heritage of liberty and self-government, but it has become the official policy of the country's ruling party and much of the American intelligentsia.

Former Clinton Labor Secretary Robert Reich responded to the news that Elon Musk was purchasing Twitter by declaring that preserving free speech online was "Musk's dream. And Trump's. And Putin's. And the dream of every dictator, strongman, demagogue, and modern-day robber baron on Earth. For the rest of us, it would be a brave new nightmare." According to Reich, censorship is "necessary to protect American democracy."

To a ruling class that had already grown tired of democracy's demand that freedom be granted to its subjects, disinformation provided a regulatory framework to replace the U.S. Constitution. By aiming at the impossible, the elimination of all error and deviation from party orthodoxy, the ruling class ensures that it will always be able to point to a looming threat from extremists—a threat that justifies its own iron grip on power.

A siren song calls on those of us alive at the dawn of the digital age to submit to the authority of machines that promise to optimize our lives and make us safer. Faced with the apocalyptic threat of the "infodemic," we are led to believe that only superintelligent algorithms can protect us from the crushingly inhuman scale of the digital information assault. The old human arts of conversation, disagreement, and irony, on which democracy and much else depend, are subjected to a withering machinery of military-grade surveillance—surveillance that nothing can withstand and that aims to make us fearful of our capacity for reason.

> *If you work in the "disinformation" or "misinformation" fields for the government or in the private sector, and are interested in discussing your experiences, you can contact me securely at jacobsiegel@protonmail.com or on Twitter @jacob__siegel. Source confidentiality is guaranteed.*

Jacob Siegel is a Tablet contributing editor. He is writing a book for Henry Holt about the rise of the Information State that will be published in 2025. He co-hosts the Manifesto! podcast with the novelist Phil Klay.

#censorship	#First Amendment	#fake news	#social media	#U.S. intelligence	#Top Ten 2023