A Guide to Understanding the Hoax of the Century

Jacob Siegel writes in *Tablet*:

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.

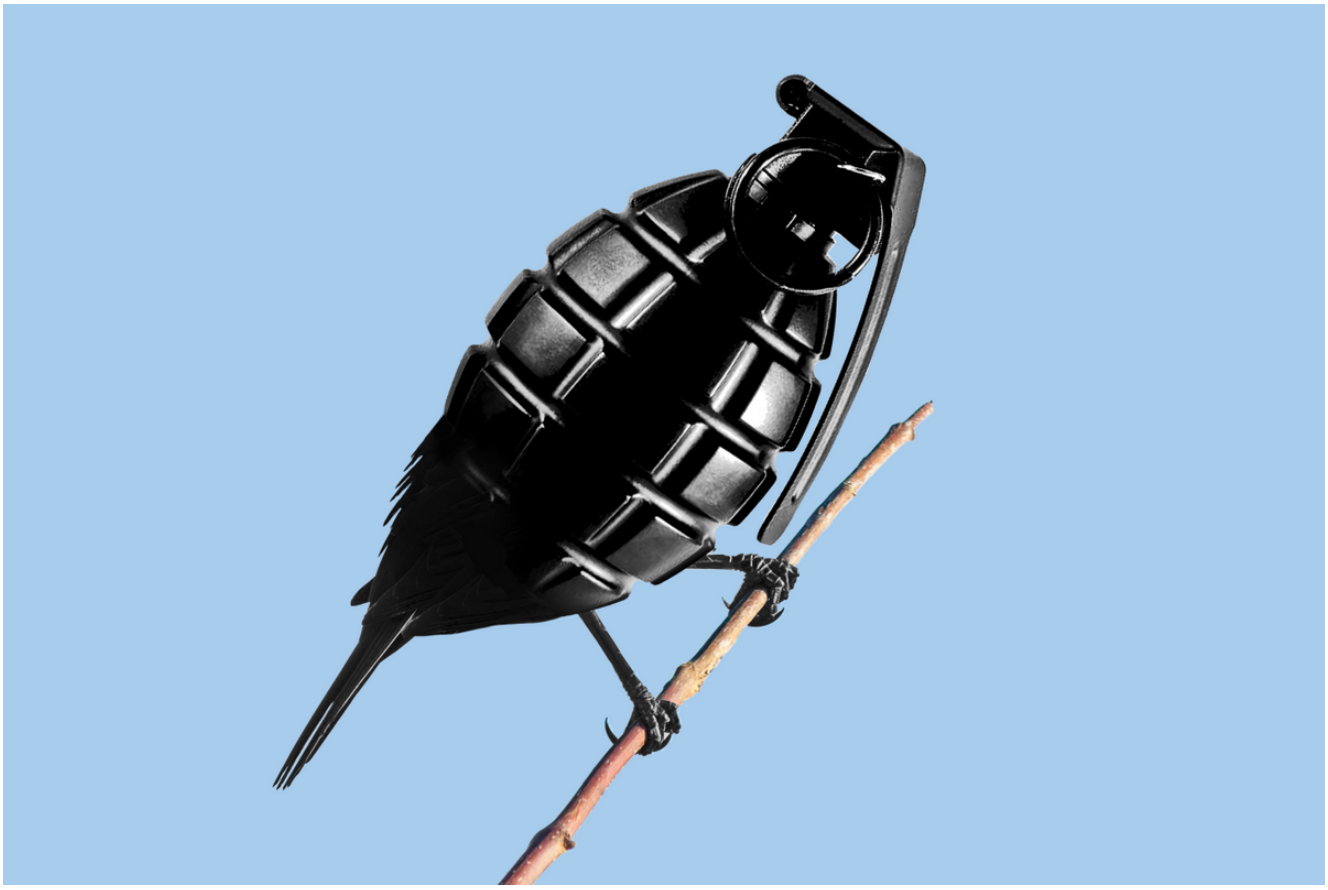
And on it went in countless articles that dominated the news cycle for the next two years.

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

Continue reading here.