What Is Disinformation?

In March 2017, the U.S. Senate Select Committee on Intelligence invited me to testify in the first open expert hearing on Russian interference in the 2016 presidential election. Committee staffers from both parties wanted me to help present to the American public the available forensic evidence that implicated Russia, evidence that at the time was still hotly contested among the wider public, and that, of course, the Russian government denied—as did the president of the United States. The situation was unprecedented.

The other two witnesses were Keith Alexander, former head of the National Security Agency, and Kevin Mandia, CEO of FireEye, a leading information security firm. Just before the hearing began, a staffer brought us from the greenroom to the witness table. Everybody else was seated already. As we walked in, I looked at the row of senators in front of us. Most of the committee members were present. Their faces looked familiar. The room was crowded; press photographers, lying on the floor with cameras slung around their necks, were soon ushered out. I envied them for a moment.

The senators sat behind a giant semicircular, heavy wooden table that seemed to encroach on the witnesses. Early on in the hearing, soon after our opening statements, Senator Mark Warner, D-VA, asked if we had "any doubt" that Russian agents had perpetrated the hack of the Democratic National Committee and the disinformation operation that took place during the campaign. He wanted a short answer. I considered my response as Mandia and Alexander spoke. The digital forensic evidence that I had seen was strong: a range of artifacts—not unlike fingerprints, bullet casings, and license plates of getaway cars at a crime scene—clearly pointed to Russian military intelligence. But despite the evidence, the offense seemed abstract, hypothetical, unreal. Then I thought of a conversation I'd had just two days earlier with an old Soviet bloc intelligence officer and disinformation engineer.

On the way to the Senate hearing in Washington, I had stopped in Boston. It was biting cold. I drove out to Rockport, a small town at the tip of Cape Ann, surrounded on three sides by the Atlantic Ocean. Ladislav Bittman had agreed to meet me at his studio there. Bittman, who died a year and a half later, was perhaps the single most important Soviet bloc defector to ever testify and write about the intelligence discipline of disinformation. A former head of the KGB's mighty disinformation unit once praised Bittman's 1972 book, *The Deception Game*, as one of the two best books on the subject.[1] Bittman had defected in 1968, before an experimental prototype of the internet was even invented, and seven years before I was born.

We spoke the entire afternoon in a calm, wood-paneled room. Bittman was bald, his face wizened, with youthful eyes. He listened carefully, paused to think, and spoke with deliberation. Indeed, Bittman's memory and his attention to detail were intimidating, and he would not answer my questions if he didn't know how. I was impressed. Bittman explained how entire bureaucracies were created in the Eastern bloc in the 1960s for the purpose of bending the facts, and how these projects were proposed, authorized, and evaluated. He outlined how he learned to mix accurate details with forged ones; that for disinformation to be successful, it must "at least partially respond to reality, or at least accepted views." He explained how leaking stolen documents had been "a standard procedure in disinformation activities" for more than half a century. He estimated that individual disinformation operations during the Cold War numbered more than ten thousand. And he brought the examples to life with stories: of a make-believe German neo-Fascist group with an oak-leaf logo, of forged Nazi documents hidden in a forest lake in Bohemia, of U.S. nuclear war plans leaked again and again all over Europe, of a Soviet master-forger flustered in a strip club in Prague. This careful and thoughtful old man taught me more about the subject of my forthcoming testimony than any technical intelligence report I had read or any digital forensic connections I could make. He made it real.[2]

★ ★ ★

In early 2016, I was in the middle of an extensive two-year technical investigation into MOONLIGHT MAZE, the first known state-on-state digital espionage campaign in history, a prolific, high-end Russian spying spree that began in the mid-1990s and never stopped. With luck and persistence, I was able to track down one of the actual servers used by Russian operators in 1998 to engineer a sprawling breach of hundreds of U.S. military and government networks. A retired systems administrator had kept the server, an old, clunky machine, under his desk at his home outside London, complete with original log files and Russian hacking tools. It was like finding a time machine. The digital artifacts from London told the story of a vast hacking campaign that could even be forensically linked to recent espionage activity. Our investigation showed the persistence and skill that large spy agencies bring to the table when they hack computer networks. Those big spy agencies that had invested in expensive technical signals intelligence collection during the Cold War seemed to be especially good at hacking—and good at watching others hack.

Then, on June 14, news of the Democratic National Committee computer network break-in hit. Among the small community of people who research high-end computer network breaches, there was little doubt, from that day forward, that we were looking at another Russian intelligence operation. The digital artifacts supported no other conclusion.

The following day, the leaking started, and the lying. A hastily created online account suddenly popped up, claiming that a "lone hacker" had stolen files from Democrats in Washington. The account published a few pilfered files as proof—indeed offering evidence that the leak was real, but not that the leaker was who they claimed. It was clear then, on June 16, that some of the world's most experienced and aggressive intelligence operators were escalating a covert attack on the United States.[3]

Over the next days and weeks, I watched the election interference as it unfolded, carefully collecting some of the digital breadcrumbs that Russian operators were leaving behind. In early July, I decided to write up a first draft of this remarkable story. I published two investigative pieces on the ongoing disinformation campaign, the first in late July 2016, on the day of the Democratic Convention, and the second three weeks before the general election. But I noticed that I was not adequately prepared for the task. I had a good grasp of digital espionage and its history, but not of disinformation —what intelligence professionals used to call "active measures."

⋆ ⋆ ⋆

We live in an age of disinformation. Private correspondence gets stolen and leaked to the press for malicious effect; political passions are inflamed online in order to drive wedges into existing cracks in liberal democracies; perpetrators sow doubt and deny malicious activity in public, while covertly ramping it up behind the scenes.

This modern era of disinformation began in the early 1920s, and the art and science of what the CIA once called "political warfare" grew and changed in four big waves, each a generation apart. As the theory and practice of disinformation evolved, so did the terms that described what was going on. The first wave of disinformation started forming in the interwar years, during the Great Depression, in an era of journalism transformed by the radio, newly cutthroat and fast-paced. Influence operations in the 1920s and early 1930s were innovative, conspiratorial, twisted—and nameless for now. The forgeries of this period were often a weapon of the weak, and some targeted both the Soviet Union and the United States at the same time.

In the second wave, after World War II, disinformation became professionalized, with American intelligence agencies leading the way in aggressive and unscrupulous operations, compounded by the lingering violence of global war. The CIA now called its blend of covert truthful revelations, forgeries, and outright subversion of the adversary "political warfare," a sprawling and ambitious term. Political warfare was deadliest in 1950s Berlin, just before the Wall went up. The Eastern bloc, by contrast, then preferred the more honest and precise name "disinformation." Whatever the phrase, the goals were the same: to exacerbate existing tensions and contradictions within the adversary's body politic, by leveraging facts, fakes, and ideally a disorienting mix of both.

The third wave arrived in the late 1970s, when disinformation became well-resourced and fine-tuned, honed and managed, lifted to an operational science of global proportions, administered by a vast, well-oiled bureaucratic machine. By then the term "active measures" was widely used in the Soviet intelligence establishment and among its Eastern bloc satellite agencies. The name stuck, and indeed was quite elegant, because it helped capture a larger conceptual and historical trend at play: after 1960, the measures were becoming progressively more active, with the East gaining an upper hand. Then the Soviet Union collapsed, and any remaining sense of ideological superiority retreated.

The fourth wave of disinformation slowly built and crested in the mid-2010s, with disinformation reborn and reshaped by new technologies and internet culture. The old art of slow-moving, highly skilled, close-range, labor-intensive psychological influence had turned high-tempo, low-skilled, remote, and disjointed. Active measures were now not only more active than ever before but less measured—so much so that the term itself became contested and unsettled.

Surviving our age of organized, professional deception requires a return to history. The stakes are enormous—for disinformation corrodes the foundation of liberal democracy, our ability to assess facts on their merits and to self-correct accordingly. That risk is old. Yet the crush of a relentless news cycle means that everything feels new, breaking, headlong; established orders appear fleeting, with views veering to the fringes, and new fissures cracking open. The crisis of our Western democracies has too often been referred to as unprecedented. This sense of novelty is a fallacy, a trap. The election interference of 2016 and the renewed crisis of the factual has a century-long prelude, and yet, unprepared and unaware, most Democrats before the 2016 election and most Republicans after the election *underestimated* and played down the risks of disinformation. Conversely, many close observers of the highly contested Special Counsel investigation of 2017 to 2019, still not fully risk-aware after the 2016 election, ended up *overestimating* and playing up the effects of an adversarial campaign that was, although poorly executed, designed to be overestimated. The best, and indeed the only, potent antidote against such pitfalls is studying the rich history of political warfare. Only by taking careful and accurate measure of the fantastic past of disinformation can we comprehend the present, and fix the future. A historical inquiry into the rise of active measures reveals a quintessentially modern story, one closely tied to the major cultural and technical trends of the past hundred years.

The twentieth century was a vast test lab of disinformation and professional, organized lying, especially during the interwar years and the Cold War, and yet Western scholars and the wider public have largely chosen to ignore the history of organized deception. Historians usually prefer telling true stories to retelling fakes. There are exceptions; several episodes have recently been well documented, for example, the tale of the Zinoviev letter,[4] a 1924 forgery that turned into a major British political scandal, or the persistent 1980s hoax that AIDS was a weapon developed by the United States Army.[5] The CIA's less aggressive cultural covert action campaign in the early Cold War is well explored, most famously the Congress of Cultural Freedom.[6] Military deception at war is also well researched.[7] But most twentieth-century disinformation operations have simply been forgotten, including some of the most extensive and successful. Twenty-first-century liberal democracies can no longer afford to neglect this past. Ignoring the rich and disturbing lessons of industrial-scale Cold War disinformation campaigns risks repeating mid-century errors that are already weakening liberal democracy in the digital age.

Recognizing an active measure can be difficult. Disinformation, when done well, is hard to spot, especially when it first becomes public. It will therefore be helpful to clarify what an active measure is, and what it is not.

First, and most important, active measures are not spontaneous lies by politicians, but the methodical output of large bureaucracies. Disinformation was, and in many ways continues to be, the domain of intelligence agencies—professionally run, continually improved, and usually employed against foreign adversaries. Second, all active measures contain an element of disinformation: content may be forged, sourcing doctored, the method of acquisition covert; influence agents and cutouts may pretend to be something they are not, and online accounts involved in the surfacing or amplification of an operation may be inauthentic. Third, an active measure is always directed toward an end, usually to weaken the targeted adversary. The means may vary: creating divisions between allied nations, driving wedges between ethnic groups, creating friction between individuals in a group or party, undermining the trust specific groups in a society have in its institutions. Active measures may also be directed toward a single, narrow objective—to erode the legitimacy of a government, for example, or the reputation of an individual, or the deployment of a weapon system. Sometimes projects are designed to facilitate a specific political decision.

These features, easily misunderstood, give rise to three widespread misconceptions about the nature of disinformation, which is generally seen as sophisticated, based on propagating false news, and occurring in the public sphere.

Almost all disinformation operations are, in fact, imperfect by design, run not by perfectionists but pragmatists. Active measures are contradictory: they are covert operations designed to achieve overt influence, secret devices deployed in public debates, carefully hidden yet visible in plain sight. This inherent tension has operational consequences. Over the decades, dirty tricksters in various intelligence agencies, Western and Eastern, have discovered that tight operational security is neither cost-effective nor desirable, for both partial and delayed exposure may actually serve the interests of the attacker. It is not an accident that disinformation played out in shifting shadows, not in pitch-black darkness. Often, at least since the 1950s, the covert aspect of a given disinformation campaign was only a veneer, imperfect and temporary by design.

Also, disinformation is not simply fake information—at least, not necessarily. Some of the most vicious and effective active measures in the history of covert action were designed to deliver entirely accurate information. In 1960, for example, Soviet intelligence produced a pamphlet that recounted actual lynchings and other gruesome acts of racial violence against African Americans from Tennessee to Texas; the KGB then distributed English and French versions of the pamphlet in more than a dozen African countries, under the cover of a fake African American activist group. In more recent memory, intelligence agencies have passed on genuine, hacked-and-leaked data to WikiLeaks. Even if no forgery was produced and no content altered, larger truths were often flanked by little lies, whether about the provenance of the data or the identity of the publisher.

Finally, disinformation operations do not always take place in public. Some highly successful active measures reached their target audience without ever being publicized in a newspaper, radio broadcast, or pamphlet, and sometimes they were more effective for that very reason. The KGB called such operations “silent” measures.[8] One of the most spectacular operations of all time was a silent measure—the Stasi-engineered outcome of West Germany's first parliamentary vote of no confidence in April 1972, which kept the chancellor in power against the odds. Private victims will find it harder to dismiss a rumor or a forgery that is never subjected to public scrutiny and criticism.

This book will extract three main arguments from the history of disinformation over the past century. The first argument is conceptual. At-scale disinformation campaigns are attacks against a liberal epistemic order, or a political system that places its trust in essential custodians of factual authority. These institutions—law enforcement and the criminal justice system, public administration, empirical science, investigative journalism, democratically controlled intelligence agencies—prize facts over feelings, evidence over emotion, observations over opinion. They embody an open epistemic order, which enables an open and liberal political order; one cannot exist without the other. A peaceful transition of power after a contested vote, for example, requires trusting an election's setup, infrastructure, counting procedures, and press coverage, all in a moment of high uncertainty and political fragility. Active measures erode that order. But they do so slowly, subtly, like ice melting. This slowness makes disinformation that much more insidious, because when the authority of evidence is eroded, emotions fill the gap. As distinguishing between facts and non-facts becomes harder, distinguishing between friend and foe becomes easier. The line between fact and lie is a continuation of the line between peace and war, domestically as well as internationally.

Disinformation operations, in essence, erode the very foundation of open societies—not only for the victim but also for the perpetrator. When vast, secretive bureaucracies engage in systematic deception, at large scale and over a long time, they will optimize their own organizational culture for this purpose, and undermine the legitimacy of public administration at home. A society's approach to active measures is a litmus test for its republican institutions. For liberal democracies in particular, disinformation represents a double threat: being at the receiving end of active measures will undermine democratic institutions—and giving in to the temptation to design and deploy them will have the same result. It is impossible to excel at disinformation and at democracy at the same time. The stronger and the more robust a democratic body politic, the more resistant to disinformation it will be—and the more reluctant to deploy and optimize disinformation. Weakened democracies, in turn, succumb more easily to the temptations of active measures.

The second argument is historical. When it comes to covert active measures, moral and operational equivalence between West and East, between democracies and non-democracies, only existed for a single decade after World War II. The CIA's skill at political warfare was significant in the 1950s, especially in Berlin, and was, in practice, on par with, or even more effective than, Soviet *dezinformatsiya*. Western intelligence agencies shunned few risks, using cutouts, front organizations, leaks, and forgeries, as well as a shrewd balance of denials and semi-denials. But just when the CIA had honed its political warfare skills in Berlin, U.S. intelligence retreated from the disinformation battlefield almost completely. When the Berlin Wall went up in 1961, it did more than block physical movement between the West and the East; it also came to symbolize an ever-sharper division: the West deescalated as the East escalated.

The third argument of this book is that the digital revolution fundamentally altered the disinformation game. The internet didn't just make active measures cheaper, quicker, more reactive, and less risky; it also, to put it simply, made active measures more active and less measured. The development of new forms of activism, and new forms of covert action, have made operations more scalable, harder to control, and harder to assess once they have been launched.

The rise of networked computers gave rise to a wider culture of hacking and leaking. A diffuse group of pro-technology, anti-intelligence activists emerged in the late 1970s, gathered momentum in the late 1990s, and would unleash torrents of raw political energy another decade after that. Early hippie activists tapped into the power of First Amendment activism in the United States, later incorporating strains of techno-utopianism, hacker subculture, cyberpunk, anarchism with a libertarian bent, anti-authoritarianism, and an obsession with encryption and anonymity. Many early crypto and anonymity activists became known as the "cypherpunks," after a famous email list by that name. The second issue of *Wired* magazine, issued in May 1993, featured three of these "crypto rebels," faces covered by white plastic masks with keys printed on their foreheads, bodies wrapped in the American flag. Ten years later, the Anonymous movement, which embodied many of the same rebellious values, would embrace nearly identical Guy Fawkes masks as its trademark. Another decade after that, Edward Snowden, the iconic intelligence leaker who likewise combined a belief in the power of encryption with far-out libertarian ideas, also appeared wrapped in the American flag on the cover of *Wired*. The movement's breathless optimism expressed itself in slogans and themes: that information wanted to be free, sources open, anonymity protected, and personal secrets encrypted by default, yet government secrets could be exposed by whistle-blowers, preferably anonymously, on peer-to-peer networks. Much of this idealism was and is positive, and in many ways, activist projects have helped strengthen information security and internet freedom.

And yet, at the fringes, this emerging subculture embraced a combination of radical transparency and radical anonymity, along with hacking-and-leaking, stealing-and-publishing—and thus created what had existed only temporarily before: the perfect cover for active measures, and not only thanks to the white noise of anonymous publication activity, from torrents to Twitter. What made the cover perfect was the veritable celebrity culture that surrounded first Julian Assange, then Chelsea Manning, and finally Edward Snowden. These self-described whistle-blowers were widely idolized as heroes, seen by their supporters as unflinching and principled in the face of oppression.

The situation was a dream come true for old-school disinformation professionals. The internet first disempowered journalism and then empowered activism. By the early 2010s, it was easier than ever to test, amplify, sustain, and deny active measures, and harder than ever to counter or suppress rumors, lies, and conspiracy theories. The internet has made open societies more open to disinformation, and foreign spies started to disguise themselves in Guy Fawkes masks. Activist internet culture shrouded what used to be a shadowy intelligence tactic in a new, star-spangled cloak of crypto-libertarianism.

The other feature that made active measures more active was a major operational innovation: by the 2010s, active measures seamlessly overlapped with covert action. Networked computers, their vulnerabilities baked in, meant that information no longer targeted only minds; it could also now target machines. It had long been possible to convince, deceive, or even buy publishers, but now their platforms could also be hacked, altered, or defaced. Machines, moreover, put up less resistance than human minds did. Active measures could even be technically amplified, by using semi-automated accounts and fully automated bots, for example. The machines created the online equivalent of the laugh track in a studio-taped TV show. Moreover, computer networks could now be breached in order to achieve effects that once required a human hand, such as manipulating or incapacitating infrastructure, logistics, or supply chains. Automation and hacking, in short, became natural extensions of the active measures playbook: exercised remotely, denied at little cost, and falling short of physical violence. The line between subversion and sabotage became blurrier, operations more easily scalable, and harder to deter. The internet, with its very own culture, created a vast new human-machine interface that appeared to be optimized for mass disinformation.

Yet it wasn't all sunshine and rainbows for aggressive intelligence agencies. Yes, manipulating malcontents and malware made measures more active. But the internet exacerbated an old problem for spies. Like all bureaucracies, secret organizations crave metrics and data, to demonstrate how well they perform in the never-ending governmental competition for resources. Naturally this show-me-the-data dynamic has long applied to disinformation as well. "The desire for speedy, easily visible, and audible success sometimes makes the intelligence service the victim of its own propaganda and disinformation," observed Bittman, the Czech defector, in the early 1970s.[9] Forty years later, by the 2010s, data had become big, engagement numbers soared, and the hunger for metrics was more ferocious than ever. Yet disinformation, by design, still resisted metrics. If more data generally meant more reliable metrics, then the internet had the reverse effect on the old art of political warfare: the metrics produced by digital disinformation were, to a significant degree, themselves disinformation. The internet didn't bring more precision to the art and science of disinformation—it made active measures less measured: harder to control, harder to steer, and harder to isolate engineered effects. Disinformation, as a result, became even more dangerous.