Active Measures: The Secret History of Disinformation & Political Warfare | Thomas Rid

May 25th, 2020

*Philosophers have only interpreted the world. The point, however, is to change it.* — Karl Marx

**INTRODUCTION**

Thomas Rid is Professor of Strategic Studies at Johns Hopkins University’s School of Advanced International Studies. Rid’s latest book, *Active Measures*, a startling history of disinformation, was published in late April 2020 with Farrar, Straus and Giroux (also in Russian, Japanese, Polish). His most recent book, *Rise of the Machines* (2016), tells the sweeping story of how cybernetics, a late-1940s theory of machines, came to incite anarchy and war (also in Chinese, Russian, German, Japanese, Turkish). His 2015 article “Attributing Cyber Attacks” was designed to explain, guide, and improve the identification of network breaches (Journal of Strategic Studies 2015). In 2013 he published the widely-read book *Cyber War Will Not Take Place*. Rid’s Ph.D. thesis, “War and Media Operations: The US Military and the Press from Vietnam to Iraq,” was the first academic analysis of the role of embedded media in the 2003 Iraq War, providing a concise history of US military public affairs management since Vietnam. Rid testified on information security in front of the U.S. Senate Select Committee on Intelligence as well as in the German Bundestag and the UK Parliament. From 2011 to 2016, Rid was a professor in the Department of War Studies at King’s College London. Between 2003 and 2010, he worked at major think tanks in Berlin, Paris, Jerusalem, and Washington, DC. Rid holds a PhD from Humboldt University in Berlin.

**WHAT IS DISINFORMATION?**

Excerpts from Rid’s Book: 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.

(1) 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.

(2) 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 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.

3 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.

4 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, 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. The CIA’s less aggressive cultural covert action campaign in the early Cold War is well explored, most famously the Congress of Cultural Freedom. Military deception at war is also well researched. 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, (1) 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, (2) 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, (3) 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 (1) sophisticated, based on (2) propagating false news, and (3) 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 lynching's 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. 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. (1) The first argument is conceptual. (1) 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.

(2) 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.

(3) 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. 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.
WHAT IS TRUTH?
Excerpts from Rid’s Book: The postwar decades had exposed a cultural tension within truth itself—or rather, between two common understandings of truth that stand in permanent opposition to each other. One is a given, positive and analytical; something is true when it is accurate and objective, when it lines up with observation, when it is supported by facts, data, or experiments. It orients itself in the present, not in the distant, mythical past or an unknowable future. Truth, in this classic sense, is inherently apolitical. Truthful observations and facts became the foundation of agreement, not conflict. The analytic truth bridged divides and brought opposing views together.
Professionals such as scientists, investigative journalists, forensic investigators, and intelligence analysts relied upon a set of shared norms designed to value cold, sober evidence over hot, emotional rhetoric. Changing one’s position in response to new data was a virtue, not a weakness. But there has always been another truth, one that corresponds to belief, not facts. Something is true when it is right, when backed up by gospel, or rooted in scripture, anchored in ideology, when it lines up with values. This truth is based in some distant past or future. Truth, in this sense, is relative to a specific community with shared values, and thus inherently political. This truth is preached from a pulpit, not tested in a lab. The style of delivery is hot, passionate, and emotional, not cold, detached, and sober. Changing one’s position is a weakness. It tends to confirm and lock in long-held views, and to divide along tribal and communal lines. These two forms of truth, of course, are exaggerations, ideals, clichés. This distinction is somewhat coarse and simplistic—nevertheless, it helps explain the logic of disinformation. The goal of disinformation is to engineer division by putting emotion over analysis, division over unity, conflict over consensus, the particular over the universal. For, after all, a democracy’s approach to the truth is not simply an epistemic question, but an existential question. Putting objectivity before ideology contributed to opening societies, and to keeping them open. Putting ideology before objectivity, by contrast, contributed to closing societies, and to keeping them closed. It is therefore no coincidence that objectivity was under near-constant assault in the ideologically torn twentieth century. Ideological certainty and a feeling of epistemic superiority would help reinterpret the factual in unexpected
ways. Already, by the late 1950s, intelligence forgeries served a larger ideological truth—for example, that the United States and its aggressive NATO alliance, armed to the teeth with nuclear missiles, were the **imperialist, capitalist oppressors**. Forgeries didn't necessarily distort this truth, but articulated it more clearly. “No reporter of any democratic press could have depicted the true backstory of the Eisenhower Doctrine in a more unvarnished way than the oil magnate himself,” wrote Neues Deutschland, East Germany’s state outlet, in its introduction to the 1957 Rockefeller forgery. The publishers of Neues Deutschland saw the United States as a capitalist, interest-driven superpower. Another example, from the summer of 1969, is Peace News and Sanity, the two British peace journals, dismissing the question of whether a leaked American war plan was forged or not, because it was “near enough to the truth.” Forgeries were like a novel that spelled out a political utopia with gleaming clarity, or a modernist painting that perfectly articulated an aesthetic form: an artificial vehicle custom-designed to communicate a larger truth. As I thought about Kopp, I wondered: What was the difference between his operational constructions and my philosophical ones? Was I falling for some active measure myself as I read postmodern philosophy by the window in my very own KW? The 1960s were a critical moment in this assault on the factual, and not only for intelligence operations. It was a decade of reckoning with the harsh legacy of World War II, of decolonization, the Holocaust, the wars in Algeria and Vietnam, and with the looming destruction of humanity in a global nuclear cataclysm that seemed only hours away at any moment. The 1960s therefore witnessed a major political, cultural, artistic, and intellectual upheaval, at the heart of which was nothing less than the nature of facts themselves. Several different strains of twentieth-century philosophy and art took issue with what they considered to be a naïve “correspondence theory” of truth: facts weren’t inalterable, according to the intellectual avant-garde; they were rooted in culture, language, systems of signs, collective perceptions, discourse, not in some inalterable structure of some independent reality. This avant-garde shunned “positivism,” “structuralism,” and “realism,” and instead examined—or “deconstructed”—how facts were created, socially constructed, scientifically built, and put to use. This new approach felt empowering, and it was. By the 1970s, postmodern thought had become more widespread on campuses, although largely confined to the humanities, to art, film, literature, and perhaps architecture. Most academic
critical theorists were, however, only studying and deconstructing the “practices” of knowledge production to shape intellectual discourse, to interpret the world. Meanwhile, in the shadows, intelligence agencies were actually producing knowledge, constructing new artifacts, shaping discourse in order to serve their tactical or strategic purposes—changing the world as they went. In 1962, the KGB upgraded Department D to Service A, and ordered intelligence agencies across the Eastern bloc to follow their lead. “A” soon came to stand for active measures. One purpose of this name change, and of this new term of art, was to overcome a counterproductive focus on facts, and indeed on non-facts. What made an active measure active was not whether a construction resonated with reality, but whether it resonated with emotions, with collectively held views in the targeted community, and whether it managed to exacerbate existing tensions—or, in the jargon of Cold War operators, whether it succeeded to strengthen existing contradictions. Shortly after defecting from Czechoslovak state security, Ladislav Bittman testified on disinformation to the U.S. Senate Committee on the Judiciary. Bittman explained why disinformation worked again and again: “Politicians or journalists wanted to believe in that disinformation message,” he told the Senate. “They confirmed their opinion.” Just five months earlier, Michel Foucault delivered his landmark inaugural lecture, “The Order of Discourse,” at the Collège de France. The iconic French philosopher and social critic considered “the opposition between true and false” as a long-established, power-wielding system of exclusion that he now revealed for what it was: historical, arbitrary, modifiable, and violent. I had been reading Foucault in Prenzlauer Berg in the mid-1990s, and after my conversation with Kopp in Brandenburg, I recalled some of what I’d read. Foucault was breaking down the barrier between analytical truth and ideological truth; so were Agayants and Wagenbreth. Could this eerie convergence of Eastern spycraft and Western thought really be just a coincidence? It took a special kind of person to work in disinformation, on both sides of the Iron Curtain. Spotting weakness in adversarial societies, seeing cracks and fissures and political tensions, recognizing exploitable historical traumas, and then writing a forged pamphlet or letter or book—all of this required officers with unusual minds. Intelligence agencies that prized secrecy, military precision, and hierarchy had to find and cultivate individuals with an opposite skill set: free and unconventional thinkers, bookworms, writers, perceptive publicists with an ability to comprehend foreign cultures. Disinformation specialists even needed a certain playful quality of mind, and to enjoy exploring and exploiting contradictions. The best disinformation operators, Kopp told me, were internal rebels. One of the HVA’s best men would sometimes “not do any work for
two days, or just read or something," but then, all of a sudden,
deliver a brilliant forged manuscript. Active measures attracted
and required precisely those creative minds who were in touch
with the intellectual zeitgeist. As if to illustrate the point, Bittman,
after his defection from East to West, became a modernist
painter. The St. Petersburg trolls were a far cry from the
professionals of Service A and the X, but even they appeared
to sense this convergence. One member of the American
Department called the IRA’s work “postmodernism in the
making,” adding that it reminded him of “Dadaism, and
surrealism.” So, what can postmodernism tell us about the
history of operational constructions? (1) First, that
disinformation works, and in unexpected ways. The fine line
between fact and forgery may be clear in the moment an
operator or an intelligence agency commits the act of
falsification—for example, in the moment when a fake
paragraph is inserted into an otherwise genuine document, or
when an unwitting influence agent is lured into casting a
parliamentary vote under false pretenses, or when a bogus
online account invites unwitting users to join a street demonstration, or shares extremist posts. But
fronts, forgeries, and fakes don’t stop there. Active measures will shape what others think, decide,
and do—and thus change reality itself. When victims read and react to forged secret documents,
their reaction is real. When the cards of an influenced parliamentary vote are counted, the result is
real. When social media users gather in the streets following a bogus event invitation, the
demonstration is real. When readers start using racial epithets offline, their views are real. These
measures are active, in the sense that operations actively and immediately change views,
decisions, and facts on the ground, in the now. (2) Second, disinformation works against itself, and
again in unexpected ways. Intelligence agencies and other disinformation actors were, again and
again, affected by their own constructions. It’s not that
analysts simply believed their own lies; it’s that operators,
driven by professional education as well as bureaucratic
logic, tended to overstate rather than understate the
value of their own disinformation work. Analysts would
write after-action reviews and project memos that justified
their efforts in terms that were clearer and more
convincing than what had happened on the ground,
where cause and effect remained entangled by design—
exacerbating existing fissures and cracks, or tapping into
existing grievances, or enhancing existing activism—all
of which meant that engineered effects were very difficult
to isolate from organic developments. Yet specialized
intelligence units had and will have metrics and data at
the ready to support their past projects and future budget
authorization requests—balloons launched, protesters
counted, forgeries printed, packages mailed, letters
received, press stories clipped, or downloads and shares
and likes and page views logged. Some disinformers of
old had long understood this problem: “I don’t think it’s
possible to measure exactly, realistically, the impact of an
“active measure,” Bittman told me in March 2017, and added that there was always a degree of guessing. “You have no reliable measurement device,” he said. Active measures, in short, were impossibly hard to measure by design. Disinformation about disinformation worsened over time. A one-off disinformation event is unlikely to achieve a given goal. By the early 1960s, some operations had begun to spread out into entire campaigns that could go on for many years, even decades. As more years and decades passed, many subtle lines that once may have demarcated fact from forgery faded until they eventually disappeared entirely. Thus, forged and engineered effects mixed with, and solidified into, actual, observable effects—like a liquid cement mix setting and turning into a firm concrete foundation. With the passing of time, reverse-engineering the delicate construction process became harder and harder. Then came the internet, with the hacking and dumping of large volumes of data and social media influence campaigns. Higher numbers and refined, real-time online metrics did not make those measurement devices more reliable, but less so. Higher numbers merely translated into higher perceived confidence in assessments, thus creating an even more seductive illusion of metrics. “Measuring the actual impact of trolling and online influence campaigns is probably impossible,” said Kate Starbird, one of the world’s leading researchers of online disinformation campaigns, who examined the influence of digital disinformation on the Black Lives Matter movement. “But the difficulty of measuring impact doesn’t mean that there isn’t meaningful impact,” she added. Online engagement figures can be staggering, and new bureaucratic politics can make these figures even more staggering. One New York Times headline in late 2017 stated, “Russian Influence Reached 126 Million Through Facebook Alone.” In reality the pre-election reach of the Internet Research Agency was far less, for two reasons: only about 37 percent of Facebook’s number of “impressions” were from before November 9, 2016 (the rest was after), and “impressions” are not engagements, only what a user may have scrolled past, perhaps absentmindedly. Facebook was then under intense political pressure, and analysts and executives decided to be as liberal as they could with the data, providing an upper limit of an estimate to Congress, for fear of being accused of lowballing the problem afterward. Many old-school journalists covering what they thought were scandalous social media figures, in turn, were either unable or unwilling to assess the data on their merits, or in the context of a history that had largely been forgotten. Online metrics, in short, created a powerful illusion, an appealing mirage—the metrics created an opportunity for more, and more convincing, disinformation about disinformation. For willfully exaggerating the effects of disinformation means exaggerating the impact of disinformation. All this is bad news for future historians. Seminars, in-person discussions, and correspondence were always fleeting and rarely archived. Yet the reach of such direct human
interactions was limited throughout the twentieth century, and many if not most magazines and published newsletters were archived somewhere. Not so in the early twenty-first century, where secure electronic communications and social media conversations are both more perishable and have a wider reach. Even inside large government bureaucracies more and more memory is lost as screens replace paper, and as files get removed or destroyed. The digital age has upended the way we preserve records, and our collective memory has already begun to corrode more quickly and more thoroughly as a result. It will therefore be even more difficult to study and reconstruct the impact of active measures in the future. The internet, contrary to a popular misconception, forgets every day, especially on ephemeral social media platforms. Suspending accounts for coordinated inauthentic behavior, for example, means hiding the main records of that behavior, and potentially assisting adversaries in hiding their tracks. Accurately gauging impact becomes harder; underestimating and overstating impact becomes easier. Active measures will thus not only blur the line between fact and fiction in the present, but also in the past, in retrospect. Active measures, third, crack open divisions by closing distinctions. It is very hard to distinguish—for an activist, for the target of an active measures campaign, even for a large organization running its own active measures—between a cunning influence agent on the one hand, and a genuine activist on the other. In theory, on an individual basis, one person is either a genuine activist or a controlled agitator, but this worldview applies only in the abstract. In practice, one individual can be both genuine and an exploited asset, a witting and unwitting collaborator at the same time. Was Philip Agee, reportedly at one point a witting KGB collaborator, unwitting when he received a forged leak that was camouflaged as coming from a legitimate U.S. government whistle-blower? This postmodern problem gets even more convoluted when applied not to an individual but to a group of people. A 50,000-person demonstration may be a genuine expression of political dissatisfaction, as with the demonstrations against NATO ballistic missiles in Germany.
Yet a large demonstration can also be exploited, organized, and even funded by an adversarial power, with, say, an interest in stopping the deployment of NATO ballistic missiles in Europe, all without undermining the legitimate character of the protest. Other examples are activist platforms and leak projects like the Fifth Estate, CyberGuerrilla, or WikiLeaks, which can empower witting participants and genuine activist projects at the same time, even in the same instance. Active measures are therefore difficult to contain conceptually, with no obvious beginning or end. The problem may not be the quality of the data or the design of the research; the problem may be the quality of an operation and the very design of the “construction” in the first place. This seeming contradiction is no contradiction, but a core feature of active measures over the past century. Active measures are purpose-designed temptations, designed to exaggerate, designed to give in to prejudice, to pre-formed notions—and to erode the capacity of an open society for fact-based, sober debate, and thus wear down the norms and institutions that resolve internal conflict peacefully.

This strange postmodern intelligence practice is, confusingly, underdetermined by observable evidence. Saying where an operation ended, and whether it failed or succeeded, requires more than facts; it requires a judgment call, which in practice means a political decision, often a collective decision. Therefore, if a targeted community believes that a disinformation campaign was a major success, then it has made it a major success. Disinformation, finally, is itself disintegrating. Bureaucratically, this degeneration proceeded with the breakup of the old Soviet security establishment and the dissolution of the once-so-formidable spy agencies of the Eastern bloc. The term “active measures” faded, even in Russia, in the early 1990s as the KGB’s First Chief Directorate was transitioned into the SVR. The sweeping official history of Russian foreign intelligence acknowledges that over the past century the designations of the same operational activity—disinformation—came and went, from “operational games” to “active measures” to the blander, more recent “support measures.”

Then came the rise of the internet, which upended the old art and science of disinformation in unexpected ways. Cutthroat media competition and distrust in “opinion factories,” as the Eastern bloc had recognized by mid-century, still worked to the advantage of disinformation operators in the mid-2010s. But the amount of craftsmanship and work required from disinformation specialists was lower in the twenty-first century than it was in the twentieth. Digital storage made it possible to breach targets remotely and extract vast amounts of compromising material. The internet facilitated acquiring and publishing unprecedented volumes of
raw files at a distance and anonymously. Automation helped to create and amplify fake personas and content, to destroy data, and to disrupt. Speed meant that operational adaptation and adjustments could take place not over years, months, or weeks—but in days, hours, even minutes. Activist culture meant existing leak platforms outperformed purpose-created ones. And the darker, more depraved corners of the internet offered teeming petri dishes of vicious, divisive ideas, and guaranteed a permanent supply of fresh conspiracy theories. All this took place while many reporters, worn down by breakneck news cycles, became more receptive to covering leaked, compromising material of questionable provenance, and as publishers recycled unoriginal, repetitive content. The end effect was that a significant and large portion of the disinformation value-creation chain was outsourced to the victim society itself, to journalists, to activists, to freelance conspiracy theorists, and, to a lesser degree, to researchers. The temptingly obvious conclusion about these trends appears to be that the art and craft of disinformation has become easier—yet such a finding would be misleading. Active measures have become more active and less measured to such a degree that they are themselves disintegrating—and this disintegration creates a new set of challenges. For the offender, campaigns have become harder to control, harder to contain, harder to steer, harder to manage, and harder to assess. For victims, disinformation campaigns have also become more difficult to manage, more difficult to assess in impact, and more difficult to counter. At the beginning of the third decade of the twenty-first century, both open and closed societies, many thrown into self-doubt and outright identity crises by the rise of the internet and its side effects, are both overstating and, more rarely, understating the threat and the potential of disinformation campaigns—and thus helping expand and escalate that very threat and its potential. This constructivist vortex is propelled by an unprecedented confluence of incentives that lead many victims—politicians, journalists, technologists, intelligence analysts, adversary operators, and most researchers—to highlight the potentials of disinformation over its limitations. Perhaps the most vivid illustration of this trend is the fantastic story of the Shadow Brokers—the devastating NSA leak with its subsequent reuse and integration of U.S. government hacking tools into the Russian Not-Petya computer worm, in the words of the White House the “most destructive and costly” computer network attack in history. That iconic overall campaign was also a disinformation project. The theft, the gradual and meticulously timed release of files, the weaponization of experts and journalists, and the subsequent destructive redeployment of computer code was designed, carefully planned, and executed with skill and discipline as an active measure—yet it has remained unclear for years who was responsible for the different components of this campaign. Whoever initiated the leak, an insider or a foreign intelligence agency, the Shadow Brokers campaign was an artful masterpiece that illustrated, in its cruel uncertainty, the twisted logic of active measures—irreversibly blurring the line between victim and perpetrator, between observation and participation, between reality and representation.
PREVIOUS BOOKS

Rise of the Machines — As lives offline and online merge even more, it is easy to forget how we got here. Rise of the Machines reclaims the spectacular story of cybernetics, one of the twentieth century’s pivotal ideas. Springing from the mind of mathematician Norbert Wiener amid the devastation of World War II, the cybernetic vision underpinned a host of seductive myths about the future of machines. Cybernetics triggered blissful cults and military gizmos, the Whole Earth Catalog and the air force’s foray into virtual space, as well as crypto-anarchists fighting for internet freedom. In Rise of the Machines (June 28, 2016), Thomas Rid draws on unpublished sources—including interviews with hippies, anarchists, sleuths, and spies—to offer an unparalleled perspective into our anxious embrace of technology.

Cyber War Will Not Take Place — "Cyber war is coming," announced a landmark RAND report in 1993. In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the "fifth domain" of warfare. This book takes stock, twenty years on: is cyber war really coming? Has war indeed entered the fifth domain? Cyber War Will Not Take Place (September 1, 2013) cuts through the hype and takes a fresh look at cyber security. Thomas Rid argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways. The threat consists of three different vectors: espionage, sabotage, and subversion. The author traces the most significant hacks and attacks, exploring the full spectrum of case studies from the shadowy world of computer espionage and weaponized code. With a mix of technical detail and rigorous political analysis, the book explores some key questions: What are cyber weapons? How have they changed the meaning of violence? How likely and how dangerous is crowd-sourced subversive activity? Why has there never been a lethal cyber attack against a country’s critical infrastructure? How serious is the threat of “pure” cyber espionage, of exfiltrating data without infiltrating humans first? And who is most vulnerable: which countries, industries, individuals?

War 2.0: Irregular Warfare in the Information Age — In this book, Rid argues that two intimately connected grassroots trends—the rise of insurgencies and the rise of the web—are putting modern armies under huge pressure to adapt new forms of counterinsurgency to new forms of social war. After the U.S. military faltered in Iraq after 2003, a robust insurgency arose. Counterinsurgency became a social form of war in which the local population was the center of gravity and public opinion at home the critical vulnerability. War 2.0 traces the contrasting ways in which insurgents & counterinsurgents have adapted irregular conflict to novel media platforms. It examines the public affairs policies of the U.S. land forces, the British Army, and the Israel Defense Forces. Then, it compares the media-related counterinsurgency methods of these conventional armies with the methods devised by their irregular adversaries, showing how such organizations as al-Qaeda, the Taliban, and Hezbollah use the web, not merely to advertise their political agenda and influence public opinion, but to mobilize a following and put violent ideas into action.
POSTMODERNISM

Postmodernism is a broad movement that developed in the mid-to-late 20th century across philosophy, the arts, architecture, and criticism, marking a departure from modernism. The term has been more generally applied to describe a historical era said to follow after modernity and the tendencies of this era. Postmodernism is generally defined by an attitude of skepticism, irony, or rejection toward what it describes as the grand narratives and ideologies associated with modernism, often criticizing Enlightenment rationality and focusing on the role of ideology in maintaining political or economic power. Postmodern thinkers frequently describe knowledge claims and value systems as contingent or socially-conditioned, describing them as products of political, historical, or cultural discourses and hierarchies. Common targets of postmodern criticism include universalist ideas of objective reality, morality, truth, human nature, reason, science, language, and social progress. Accordingly, postmodern thought is broadly characterized by tendencies to self-consciousness, self-referentiality, epistemological and moral relativism, pluralism, and irreverence. Postmodern critical approaches gained purchase in the 1980s and 1990s and have been adopted in a variety of academic and theoretical disciplines, including cultural studies, philosophy of science, economics, linguistics, architecture, feminist theory, and literary criticism, as well as art movements in fields such as literature, contemporary art, and music. Postmodernism is often associated with schools of thought such as deconstruction, post-structuralism, and institutional critique, as well as philosophers such as Jean-François Lyotard, Jacques Derrida, and Fredric Jameson. Criticisms of postmodernism are intellectually diverse and include arguments that postmodernism promotes obscurantism, is meaningless, and that it adds nothing to analytical or empirical knowledge.

CYBERNETICS

Cybernetics is a transdisciplinary approach for exploring regulatory systems—their structures, constraints, and possibilities. Norbert Wiener defined cybernetics in 1948 as "the scientific study of control and communication in the animal and the machine." In other words, it is the scientific study of how humans, animals and machines control and communicate with each other. Cybernetics is applicable when a system being analyzed incorporates a closed signaling loop—originally referred to as a "circular causal" relationship—that is, where action by the system generates some change in its environment and that change is reflected in the system in some manner (feedback) that triggers a system change. Cybernetics is relevant to, for example, mechanical, physical, biological, cognitive, and social systems. The essential goal of the broad field of cybernetics is to understand and define the functions and processes of systems that have goals and that participate in circular, causal chains that move from action to sensing to comparison with desired goal, and again to action. Its focus is how anything (digital, mechanical or biological) processes information, reacts to information, and changes or can be changed to better accomplish the first two tasks. Cybernetics includes the study of feedback, black boxes and derived concepts such as communication and control in living organisms, machines and organizations including self-organization. Concepts studied by cyberneticists include, but are not limited to: learning, cognition, adaptation, social control, emergence, convergence, communication, efficiency, efficacy, and connectivity. In cybernetics these concepts (otherwise already objects of study in other disciplines such as biology and engineering) are abstracted from the context of the specific organism or device. Contemporary cybernetics began as an interdisciplinary study connecting the fields of control systems, electrical network theory, mechanical engineering, logic modeling, evolutionary biology, neuroscience, anthropology, and psychology in the 1940s. System dynamics, originated with applications of electrical engineering control theory to other kinds of simulation models (especially business systems) by Jay Forrester at MIT in the 1950s, is a related field.
QUESTIONS

**Background** — Tell us a bit about your background. Q: What led you to write this book? Q: How does “Active Measures” fit into the linear progression of your intellectual development?

**Research** — Q: What kind of research did you do for this book? Q: How did you go about doing the research?

**Active Measures vs. Disinformation** — Q: What are active measures? *** Ladislav Bittman describes them as “systematic deception” meant to change behavior or illicit a particular response. Q: What are the goals of active measures?

**Espionage vs. Disinformation** — Q: What is the difference between espionage & disinformation? Q: What made you realize that you didn’t actually understand active measures?

**Birth of Disinformation** — Q: Why did the history of disinformation begin in the early 1920’s? Q: What was it about that period? Q: Where did it begin?

**Effectiveness of Active Measures** — Q: Is one of the aspects that makes active measures so effective its ability to exploits the hypocrisies of the attackers and the attacked? (e.g. the fact that our own government is engaged in many morally dubious actions, while simultaneously claiming moral superiority in its condemnation of others for similar acts) Q: Is it the “use of truth in the service of lies,” that makes disinformation more effective? You can’t understand cyber operations in the 21st century without first understanding intelligence operations in the 21st century. — Thomas Rid

**Role of Journalistic Establishment in AM** — Q: What is the relationship between journalists and the intelligence agencies implementing active measures? Q: How should journalists navigate this liminal space?

**Active Measures in the Internet Age** — Q: How has the Internet altered the way that active measures and disinformation are conducted?

**Dangers of Disinformation to Both Parties** — Q: What are the dangers posed by the conduct of disinformation and active measures campaigns, both to the attacker as well as to the victim?

**Truth & Postmodernism** — Q: How do we assess facts when our notions of truth have themselves come into question? Q: How do we achieve political consensus without agreed upon frameworks for verifiability?

**Conspiracy Theories** — Q: What are some examples of currently active measures? Q: Where does the so-called “Russian Hacking” fall within the framework discussed today?

**Overstating the Power of Disinformation** — Q: How do we grapple with the implications of active measures? Are overstating their power?

**Contradictions** — Q: What are the role of contradictions and exacerbating contradictions?

**Big Questions Raised** — Q: What are the big questions that your work and research raises?

**Ongoing Campaigns** — Q: What are the ongoing disinformation campaigns? Q: How do we spot such measures in real time?